



Contract # AR2479

# STATE OF UTAH COOPERATIVE CONTRACT

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

Dayl Solutions  
 \_\_\_\_\_  
 Name  
1751 Pinnacle Drive Suite 425  
 \_\_\_\_\_  
 Address  
McLean VA 22102  
 \_\_\_\_\_  
 City State Zip

LEGAL STATUS OF CONTRACTOR

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

Contact Person Sean Wilson Phone #703-270-0614 Email sean@daylsolutions.com  
 Vendor #VC0000188653 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: 09/09/2016 Termination Date: 09/08/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.
5. Administrative Fee, as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.
6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including that attached Exhibits  
 ATTACHMENT B: Scope of Services Awarded to Contractor  
 ATTACHMENT C: Pricing Discounts and Pricing Schedule  
 ATTACHMENT D: Contractor's Response to Solicitation #CH16012  
 ATTACHMENT E: SLA and Customer License Terms for AWS
- 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**  
  
 \_\_\_\_\_  
 Contractor's signature Date

**STATE**  
  
 \_\_\_\_\_  
 Director Division of Purchasing Date

Luis Benavidas CEO  
 \_\_\_\_\_  
 Type or Print Name and Title

<u>Christopher Hughes</u>	<u>801-538-3254</u>	<u>christopherhughes@utah.gov</u>
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<sup>1</sup> ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits<sup>2</sup> to the Master Agreement;
- (3) The Solicitation;
- (4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
- (5) A Service Level Agreement issued against the Participating Addendum.

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

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

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

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

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

---

<sup>1</sup> A Sample Participating Addendum will be published after the contracts have been awarded.

<sup>2</sup> The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and SaaS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**6. Discount Guarantee Period:** All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the

immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

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

**8. Confidentiality, Non-Disclosure, and Injunctive Relief**

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

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

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

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

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

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

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

## **10. Defaults and Remedies**

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

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



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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

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

**12. Force Majeure:** Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual

capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

### **13. Indemnification**

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

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

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

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

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

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

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

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be

responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

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

**15. Individual Customers:** Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

## **16. Insurance**

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

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

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

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	<b>Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions</b> 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<sup>3</sup>.

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.

---

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

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

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

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

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

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

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

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

**25. Purchasing Entity Data:** Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata. Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or



sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

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

## **26. Records Administration and Audit.**

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

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

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

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

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

Additionally, some states may require an additional administrative fee be paid directly to

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

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

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

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

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

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

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

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

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

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

f. The Contractor warrants that the Products it provides under this Master Agreement

are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

### **32. Transition Assistance:**

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

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

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

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

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

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

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

### **37. Governing Law and Venue**

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

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

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

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

**38. No Guarantee of Service Volumes:** The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition

as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

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

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

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

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

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

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

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

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

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

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

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

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

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

## **Exhibit 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

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

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
SaaS: <i>Infor-CloudSuite for Public Sector</i> <ul style="list-style-type: none"> <li>• <i>Financial management and procurement</i></li> <li>• <i>Human Resources and payroll</i></li> <li>• <i>Public Safety</i></li> <li>• <i>Libraries</i></li> </ul>	X	X	X	Public
*IaaS: <b>Compute:</b> <ul style="list-style-type: none"> <li>• <i>EC2</i></li> <li>• <i>EC2 Container Services</i></li> <li>• <i>EC2 Container Registry</i></li> <li>• <i>Auto Scaling</i></li> <li>• <i>Elastic Load Balancing(ELB)</i></li> <li>• <i>VPC</i></li> </ul> <b>Storage:</b> <ul style="list-style-type: none"> <li>• <i>S3</i></li> <li>• <i>CloudFront</i></li> <li>• <i>Elastic Block Storage (EBS)</i></li> <li>• <i>Glacier</i></li> <li>• <i>Elastic File System</i></li> </ul>	X	X	X	Public, Private, Hybrid

<ul style="list-style-type: none"> <li>• <i>Import/Export Snowball</i></li> <li>• <i>Storage Gateway</i></li> </ul> <p><b>Database:</b></p> <ul style="list-style-type: none"> <li>• <i>RDS (Managed Database Service)</i></li> <li>• <i>Elastic Cache</i></li> <li>• <i>DynamoDB</i></li> <li>• <i>Redshift</i></li> <li>• <i>Migration Services</i></li> </ul> <p><b>Network:</b></p> <ul style="list-style-type: none"> <li>• <i>Direct Connect</i></li> <li>• <i>Route 53</i></li> </ul> <p><b>Developer Tools:</b></p> <ul style="list-style-type: none"> <li>• <i>CodeCommit</i></li> <li>• <i>CodeDeploy</i></li> <li>• <i>CodePipeline</i></li> <li>• <i>Command Line Tool</i></li> </ul> <p><b>Management Tools:</b></p> <ul style="list-style-type: none"> <li>• <i>CloudWatch</i></li> <li>• <i>CloudFormation</i></li> <li>• <i>CloudTrail</i></li> <li>• <i>Config</i></li> <li>• <i>OpsWork</i></li> <li>• <i>Management Console</i></li> <li>• <i>Service Catalog</i></li> <li>• <i>Trusted Advisor</i></li> <li>• <i>Inspector</i></li> </ul> <p><b>Security &amp; Identity:</b></p> <ul style="list-style-type: none"> <li>• <i>Identity &amp; Access Management (IAM)</i></li> <li>• <i>CloudHSM</i></li> <li>• <i>Certificate Manager</i></li> <li>• <i>WAF</i></li> </ul>				
---	--	--	--	--

<ul style="list-style-type: none"> <li>• <i>Key Management Service</i></li> <li>• <i>Directory Service</i></li> </ul> <p><b>Analytics:</b></p> <ul style="list-style-type: none"> <li>• <i>EMR</i></li> <li>• <i>Data Pipeline</i></li> <li>• <i>Kinesis</i></li> <li>• <i>Machine Learning</i></li> <li>• <i>QuickSight</i></li> <li>• <i>Elasticsearch Service</i></li> </ul> <p><b>Internet of Things:</b></p> <ul style="list-style-type: none"> <li>• <i>IoT</i></li> </ul> <p><b>Application Services:</b></p> <ul style="list-style-type: none"> <li>• <i>API Gateway</i></li> <li>• <i>SNS</i></li> <li>• <i>SQS</i></li> <li>• <i>SES</i></li> <li>• <i>SWF</i></li> <li>• <i>CloudSearch</i></li> <li>• <i>AppStream</i></li> <li>• <i>Elastic Transcoder</i></li> </ul> <p><b>Mobile Services:</b></p> <ul style="list-style-type: none"> <li>• <i>Mobile SDK</i></li> <li>• <i>Mibile Hub</i></li> <li>• <i>Cognito</i></li> <li>• <i>Mobile Analytics</i></li> </ul> <p><b>Enterprise Applications:</b></p> <ul style="list-style-type: none"> <li>• <i>WorkSpaces</i></li> <li>• <i>WorkDocs</i></li> <li>• <i>Workmail</i></li> </ul> <p><b>Marketplace Solutions:</b></p> <ul style="list-style-type: none"> <li>• <i>AWS Marketplace</i></li> </ul>				
<p>PaaS:</p> <p><i>Amazon Web Services</i></p> <ul style="list-style-type: none"> <li>• <i>Elastic BeanStalk</i></li> </ul>	X	X	X	Public, Private, Hybrid

• <i>AWS Lambda</i>				
---------------------	--	--	--	--

\*Note: Depending on the use-case, end-user requirements and configuration models, many of the services listed in IaaS may crossover to other service models.

# Attachment <sup>c</sup> Cost Schedule

---

## Solicitation Number CH16012 NASPO ValuePoint Cloud Solutions RFP

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

<b>Software as a Service</b>	<b>Discount % - 2% off AWS PaaS Products</b>
<b>Infrastructure as a Service</b>	<b>Discount % - 2% off AWS PaaS Products</b>
<b>Platform as a Services</b>	<b>Discount % - 2% off AWS PaaS Products</b>
<b>Value Added Services</b>	<b>Discount % - 0</b>

---

### **Additional Value Added Services:**

#### **Maintenance Services**

**Onsite Hourly Rate \$ - See Cost Proposal (Section 1.10 Maintenance and Support)**

**Remote Hourly Rate \$ - See Cost Proposal (Section 1.10 Maintenance and Support)**

#### **Professional Services**

- **Deployment Services**
  - i. **Onsite Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**
  - ii. **Remote Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**
  
- **Consulting/Advisory Services**
  - i. **Onsite Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**
  - ii. **Remote Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**
  
- **Architectural Design Services**
  - i. **Onsite Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**
  - ii. **Remote Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**
  
- **Statement of Work Services**
  - i. **Onsite Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**

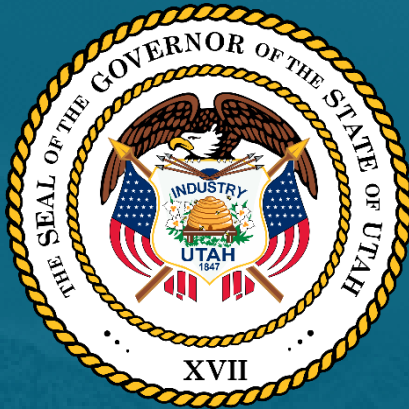
- ii. Remote Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**

**Partner Services**

- i. Onsite Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**
- ii. Remote Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**

**Training Deployment Services**

- i. Onsite Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**
- ii. Online Hourly Rate \$ - See Cost Proposal (Section 1.11 Professional & Consulting Services)**



State of Utah Division of Purchasing

# NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTION

CH16012

## COST PROPOSAL





# Contents

1.0	Cost Proposal [RFP Section 9] .....	2
1.1	Hosting (Compute & Networking).....	3
1.1.1	Instance Types .....	3
1.2	Amazon WorkSpace .....	7
1.3	Amazon WorkDocs .....	7
1.4	Amazon WorkMail (Preview) .....	8
1.5	GIS SaaS (Software as a Service) .....	8
1.6	Database Services .....	8
1.7	DB Instances (Bring Your Own License or BYOL) .....	10
1.8	Non-Relational Database .....	11
1.9	Storage .....	11
1.10	Data Transfer.....	13
1.11	All Other Cloud Services & Solutions.....	13
1.12	Infor SaaS Products .....	17
1.13	Data Analytics.....	35
1.14	Maintenance and Support .....	36
1.15	Professional & Consulting Services .....	37
1.16	Other Non-Recurring Costs .....	38
1.17	Cost Schedule Assumptions .....	39
2.0	Appendix A – Sample Infor SaaS Agreement.....	0

## 1.0 Cost Proposal [RFP Section 9]

*Cost Proposals will be evaluated independently from the technical proposal. Offeror's cost proposal must include the items discussed in Section 9 of the RFP. Cost will be evaluated independently from the Mandatory Minimum Requirements, and the Technical responses. Inclusion of any cost or pricing data within the Detailed Technical Proposal will result in the proposal being judged as non-responsive for violation of UCA § 63G-6a-707(5). All costs incurred by an Offeror in the preparation and submission of a proposal, including any costs incurred during interviews, oral presentations, and/or product demonstrations are the responsibility of the Offeror and will not be reimbursed by the Lead State or NASPO ValuePoint.*

Given that technology products generally depreciate over time and go through typical product lifecycles, it is more favorable for Purchasing Entities to have the Master Agreement be based on minimum discounts off the Offeror's commercially published pricelists versus fixed pricing. In addition, Offerors will have the ability to update and refresh their respective price books, as long as the agreed-upon discounts are fixed. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

Offeror must identify its cost proposal, Attachment G, as "Cost Proposal – CH16012 Cloud solutions". No specific format is required for an Offeror's price schedule; however the Offeror must provide and list a discount from its pricing catalog. New discount levels may be offered for new services that become available during the term of the Master Agreement, as allowed by the Lead State.

Pricing catalogs should include the price structures of the cloud solutions models and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing must be all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

The Lead State understands that each Offeror may have its own pricing models and schedules for the Services described in the RFP. It is the intent of the RFP to allow price schedules that are viewed in the traditional line item structure or price schedule that have pay-as-you-go characteristics.

An Offeror's price catalog should be clear and readable. Participating Entities, in reviewing an Offeror's Master Agreement, will take into account the discount offered by the Offeror along with the transparent, publicly available, up-to-date pricing and tools that will allow customers to evaluate their pricing.

Individual Participating Addendums will use the cost proposals pricing as a base and may negotiate an adjusted rate.

Offeror's price catalog should be broken into category for each service category. For example if an Offeror provides a SaaS offering then its price catalog should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

Some Participating Entities may desire to use an Offeror for other related application modifications to optimize or deploy cloud solutions applications. Responses to the RFP must include hourly rates by job specialty for use by Participating Entities for these types of database/application administration, systems engineering & configuration services and consulting throughout the contract period. The hourly rates should be a fully burdened rate that includes labor, overhead, and any other costs related to the service. The specific rate (within a range) charged for

each proposed contracted service would be the lowest rate shown unless justified in writing and approved by the Lead State. Any of these valued-added services must be included in your cost proposal, e.g., by an hourly rate.

In an effort to continually provide our customers with a simple process of provisioning cloud services, Day1 has taken steps to reduce the complexity of price evaluations by offering a percentage (2%) discount off MSRP for Amazon Web Services (AWS) services and products authorized under our APN agreements. Also, as monthly price reductions are implemented by AWS, we immediately pass on those savings to our end-clients.

Up-to-date MSRP pricing for Amazon Web services is found by at <http://aws.amazon.com/pricing/>.

The Maintenance and Support section of this cost schedule has been updated. AWS Business Support is provided to all customers at MSRP. Customers also have the option to choice Day1 Standard, Premium or Managed Services.

## 1.1 Hosting (Compute & Networking)

### 1.1.1 Instance Types

The instances detailed following tables are available in a choice of instance types designed to handle various application and workload needs. MSRP Instance pricing depends on Instance type, pricing model (On-Demand, Reserved, or Spot), Region, designated or non-designated hardware, operating system, and, optionally, database or software inclusions. Note: In some cases, not all instance type availability may vary by Region or other option.

Type	Virtual CPUs	Elastic Compute Units	Memory (GiB)
<b>General Purpose – Current Generation</b>			
t2.micro	1	Variable	1
t2.small	1	Variable	2
t2.medium	2	Variable	4
m3.medium	1	3	3.75
m3.large	2	6.5	7.5
m3.xlarge	4	13	15
m3.2xlarge	8	26	30
m4.large	2		8
m4.xlarge	4		16
m4.2xlarge	8		32
m4.4xlarge	16		64
m4.10xlarge	40		160
<b>Compute Optimized – Current Generation</b>			
c3.large	2	7	3.75
c3.xlarge	4	14	7.5
c3.2xlarge	8	28	15
c3.4xlarge	16	55	30

Type	Virtual CPUs	Elastic Compute Units	Memory (GiB)
c3.8xlarge	32	108	60
c4.large	2		3.75
c4.xlarge	4		7.5
c4.2xlarge	8		15
c4.4xlarge	16		30
c4.8xlarge	36		60
<b>Memory Optimized – Current Generation</b>			
r3.large	2	6.5	15
r3.xlarge	4	13	30.5
r3.2xlarge	8	26	61
r3.4xlarge	16	52	122
r3.8xlarge	32	104	244
<b>Storage Optimized – Current Generation</b>			
i2.xlarge	4	14	30.5
i2.2xlarge	8	27	61
i2.4xlarge	16	53	122
i2.8xlarge	32	104	244
<b>GPU Instances – Current Generation</b>			
g2.2xlarge	8	26	15
g2.8xlarge	32		60
<b>Dense Storage – Current Generation</b>			
d2.xlarge	4		30.5
d2.2xlarge	8		61
d2.4xlarge	16		122
d2.8xlarge	36		244

### On Demand Instances

On-Demand Instances let you pay for compute capacity by the hour with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs. Pricing is per instance-hour consumed for each instance, from the time an instance is launched until it is terminated. Each partial instance-hour consumed will be billed as a full hour.

Application Hosting	AWS EC2 Compute Resources 2.0 % off MSRP
Windows Usage	All Regions
Linux Usage	All Regions
Red Hat Enterprise Linux Usage	Public Cloud
SUSE Linux Enterprise Server Usage	Public Cloud

*\*All instances include RAM, CPU and Operating System.*

### 1.1.1.1 New Reserved Instance Model

There is now a single type of Reserved Instance and it has three payment options. All of the options continue to provide capacity assurance and discounts that are typically around 63% for a three year term when compared to On-Demand prices.

There are three payment options so that you can decide how you would like to pay for your Reserved Instance throughout the term (in descending order of effective discount):

- **All Upfront** - You pay for the entire Reserved Instance term (one or three years) with one upfront payment and get the best effective hourly price when compared to On-Demand.
- **Partial Upfront** - You pay for a portion of the Reserved Instance upfront, and then pay for the remainder over the course of the one or three year term. This option balances the RI payments between upfront and hourly.
- **No Upfront** - You pay nothing upfront but commit to pay for the Reserved Instance over the course of the Reserved Instance term, with discounts (typically about 30%) when compared to On-Demand. This option is offered with a one-year term.

Application Hosting	AWS EC2 Compute Resources 2.0 % off MSRP
Windows Usage	All Regions
Linux Usage	All Regions
Red Hat Enterprise Linux Usage	Public Cloud
SUSE Linux Enterprise Server Usage	Public Cloud

*\*All instances include RAM, CPU and Operating System.*

### 1.1.1.2 Dedicated Instances

Dedicated Instances are instances that run on hardware dedicated to a single customer. Dedicated Instances let you take full advantage of on-demand elastic provisioning, pay only for what you use, and utilize a private, isolated virtual network, all while ensuring that your compute instances will be isolated at the hardware level.

Hosting	AWS EC2 Compute Resources 2.0 % off MSRP
Windows Usage	All Regions
Linux Usage	All Regions
Red Hat Enterprise Linux Usage	Public Cloud
SUSE Linux Enterprise Server Usage	Public Cloud

*\*All instances include RAM, CPU and Operating System.*

### 1.1.1.3 Spot Instances

Spot Instances enable you to bid for unused Amazon EC2 capacity. Instances are charged the Spot Price, which fluctuates depending on the supply of and demand for Instance capacity at the time of purchase.

Hosting	AWS EC2 Compute Resources 2.0 % off MSRP
Windows Usage	All Regions
Linux Usage	All Regions
SUSE Linux Enterprise Server Usage	Public Cloud

*\*All instances include RAM, CPU and Operating System.*

### 1.1.1.4 Instances with Database Hosting

EC2 Instances configured with Microsoft SQL Server Standard or Web are available.

Application and Database Hosting	AWS EC2 Compute Resources 2.0 % off MSRP
<b>On Demand Instances</b>	<b>Availability</b>
Windows with SQL Server Standard	All Regions
Windows with SQL Server Web	All Regions
<b>Reserved Instances</b>	<b>Availability</b>
Windows with SQL Server Standard	All Regions

Application and Database Hosting	AWS EC2 Compute Resources 2.0 % off MSRP
Windows with SQL Server Web	All Regions

*\*All instances include RAM, CPU and Operating System.*

## 1.2 Amazon WorkSpace

Amazon WorkSpaces offers you an easy way to provide a fully managed, cloud-based desktop experience to your end-users. You don't have to worry about procuring or deploying hardware or installing complex software; Amazon WorkSpaces takes care of all the heavy lifting of managing hardware and software, and tasks such as patching and maintenance, enabling you to deliver a high quality desktop experience to your users.

AWS Workspace	AWS EC2 Compute Resources 2.0 % off MSRP
Workspace Bundles	Availability
Standard	Public Cloud
Standard Plus	Public Cloud
Performance	Public Cloud
Performance Plus	Public Cloud

## 1.3 Amazon WorkDocs

Amazon WorkDocs offers you an easy way to provide a fully managed, cloud-based document storage and sharing service for your employees. Amazon WorkDocs costs \$5 per month per user and includes 200 GB of storage for each user with no upfront fees or commitments. Amazon WorkDocs enables you to share and edit documents across your users fast and securely without the need of sending documents after each revision.

AWS WorkDocs	AWS EC2 Compute Resources 2.0 % off MSRP
WorkDocs Bundles	Availability
Standard	Public Cloud
Standard Plus	Public Cloud
Performance	Public Cloud
Performance Plus	Public Cloud

## 1.4 Amazon WorkMail (Preview)

Amazon WorkMail offers you a secure, managed business email, and calendar service with support for existing desktop and mobile email clients based out of the cloud. This highly sync-able email service allows for high functionality and administrative tools through the cloud. Amazon WorkMail can also be extremely fast and secure with integration with your existing corporate directory and control both the keys that encrypt all of the data.

AWS WorkMail	AWS EC2 Compute Resources 2.0 % off MSRP
WorkMail Bundles	Availability
Standard	Public Cloud
Standard Plus	Public Cloud
Performance	Public Cloud
Performance Plus	Public Cloud

## 1.5 GIS SaaS (Software as a Service)

GIS Software Only			
	Monthly	3 months	Annually
<b>Esri ArcGIS for Server Enterprise Standard</b> Up to 4 Cores (Windows and Linux)	\$2,300.00	\$ 6,000	\$ 12,000
<b>Esri ArcGIS for Server Enterprise Advanced</b> Up to 4 Cores (Windows and Linux)	\$4,700.00	\$ 12,000	\$ 24,000
Open Source			
<b>Boundless</b> Up to 4 Cores	\$ 999.00	N/A	\$8,000.00/\$16,000
Up to 4 Cores	\$ 999.00	N/A	\$8,000.00/\$16,000
Bring your own license (BYOL)			
Must select server/instance type from above.			

## 1.6 Database Services

Database Hosting in the cloud provides a number of database alternatives for developers. You can run fully managed relational and MySQL services or you can operate your own database in the cloud. Relational Database Service (RDS) is a web service that makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-



efficient and resizable capacity while managing time-consuming database administration tasks, freeing you up to focus on your applications and business.

On-Demand DB Instances let you pay for compute capacity by the hour; your DB Instance runs with no long-term commitments. This frees you from the costs and complexities of planning, purchasing, and maintaining hardware and transforms what are commonly large fixed costs into much smaller variable costs.

With Reserved Instances, you can make a low, one-time, up-front payment for each DB Instance you wish to reserve for a 1 or 3 year term. In return, you receive a significant discount off the ongoing hourly usage rate for the DB Instance(s) you reserve. Amazon RDS provides three RDS Reserved Instance types (Light, Medium, and Heavy Utilization Reserved Instances) that give you the flexibility to choose the right pricing option depending on your usage requirements.

Amazon RDS for MariaDB gives you full access to all the capabilities of the MariaDB database engine. This means that the code, applications, and tools you already use today with your existing MariaDB databases can be used with your Amazon RDS MariaDB database. Amazon RDS automatically patches the database software and backs up your database, storing the backups for a retention period you define and enables point-in-time recovery. You benefit from the flexibility of being able to scale the compute resources or storage capacity associated with your Database Instance (DB Instance) via a single API call.

AWS Database Migration Service can migrate your data to and from all widely used commercial and open-source databases. The service supports homogenous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora or Microsoft SQL Server to MySQL.

Relational Database Hosting (license Included)	AWS Database Resources 2.0 % off MSRP
<b>On-Demand Standard Deployment</b>	
MySQL	All Regions
PostgreSQL	All Regions
Oracle	All Regions
SQL Server (Express, Web, Standard)	All Regions

*Under the "License Included" service model, you do not need separately purchased Microsoft SQL Server licenses. "License Included" pricing is inclusive of software, underlying hardware resources, and Amazon RDS management capabilities. Standard DB Instance deployed in a single Availability Zone.*

<b>On-Demand Multi-AZ Deployment</b>	
MySQL	All Regions
PostgreSQL	All Regions

Relational Database Hosting (license Included)	AWS Database Resources 2.0 % off MSRP
Oracle	All Regions
<i>When you run your DB Instance as a Multi-AZ deployment for enhanced data durability and availability, Amazon RDS provisions and maintains a standby in a different Availability Zone for automatic failover in the event of a scheduled or unplanned outage.</i>	
Reserved Standard Deployment	
MySQL	All Regions
PostgreSQL	All Regions
Oracle	All Regions
SQL Server (Express, Web, Standard)	All Regions
Reserved Multi-AZ Deployment	
MySQL	All Regions
PostgreSQL	All Regions
Oracle	All Regions
<i>When you run your DB Instance as a Multi-AZ deployment for enhanced data durability and availability, Amazon RDS provisions and maintains a standby in a different Availability Zone for automatic failover in the event of a scheduled or unplanned outage.</i>	
Amazon RDS for MariaDB	
	All Regions
AWS Database Migration Services	
	US East (N. Virginia Region)

## 1.7 DB Instances (Bring Your Own License or BYOL)

Microsoft's [License Mobility](#) program (referred to henceforth as Bring Your Own License or "BYOL") allows customers who already own SQL Server licenses to run SQL Server deployments on Amazon RDS. This benefit is available to Microsoft Volume Licensing (VL) customers with SQL Server licenses (currently including Standard and Enterprise Editions) covered by active Microsoft Software Assurance (SA) contracts. The Microsoft License Mobility program is suited for customers who prefer to use existing SQL Server licenses or purchase new licenses directly from Microsoft or any other reseller. To run a DB Instance under the BYOL model, you must meet the eligibility

requirements and follow the Sign Up process laid out [here](#). You must also have the appropriate SQL Server licenses with Software Assurance for the DB Instance class and SQL Server edition you wish to run, and must adhere to Microsoft's [licensing policies](#).

Under the Bring Your Own License (“BYOL”) model, you can run Amazon RDS using your existing Oracle Database software licenses. You can also purchase Oracle Database licenses directly from Oracle and run them on Amazon RDS. To run a DB Instance under the BYOL model, you must have the appropriate Oracle Database license (with Software Update License & Support) for the DB Instance class and Oracle Database edition you wish to run. You must also follow Oracle's policies for licensing Oracle Database software in the cloud computing environment. DB Instances reside in the Amazon EC2 environment, and Oracle's licensing policy for Amazon EC2 is located [here](#).

## 1.8 Non-Relational Database

DynamoDB is a fast, fully managed NoSQL database service that makes it simple and cost-effective to store and retrieve any amount of data, and serve any level of request traffic. All data items are stored on Solid State Drives (SSDs), and are replicated across 3 Availability Zones for high availability and durability.

Non-Relational Database Hosting	AWS EC2 Compute Resources 2.0 % off MSRP
<b>Reserved Capacity</b>	<b>Availability</b>
Index Data Store	All Regions
Reserve	All Regions

## 1.9 Storage

We offer multiple storage and backup service options including basic, archival, and reduced redundancy. Amazon's **Simple Storage Service (S3)** is a simple web service that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. S3 has 99.999999999% durability, and 99.99% availability. **Reduced Redundancy** is a storage option that enables customers to reduce their costs by storing non-critical, reproducible data at lower levels of redundancy than with standard S3. Reduced redundancy storage has 99.99% durability over a given year. **Glacier** provides an extremely low-cost storage service that provides secure and durable storage for data archiving and backup. **Storage Gateway** is a service connecting an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an organization's on-premises IT environment and cloud storage infrastructure.

Simple Storage Service	
On Demand, Prices Per GB - (Standard or Reduced Redundancy)	
All Region Availability	
First 1 TB	2% off MSRP

<b>Simple Storage Service</b>	
Next 49 TB	2% off MSRP
Next 450 TB	2% off MSRP
Next 500 TB	2% off MSRP
Next 4000 TB	2% off MSRP
Over 5000 TB	2% off MSRP
<b>Fixed Price, 1 year term - (Standard or Reduced Redundancy)</b>	
<b>GovCloud Only</b>	
25 TB average per month	2% off MSRP
50 TB average per month	2% off MSRP
500 TB average per month	2% off MSRP
1000TB average per month	2% off MSRP
5000TB average per month	2% off MSRP
<b>Glacier Storage</b>	
<b>All Region Availability</b>	
Glacier Storage per GB per month	2% off MSRP
UPLOAD and RETRIEVAL, per 1000 requests	2% off MSRP
LISTVAULTS, GETJOBOUTPUT, DELETE and all other Requests	No additional cost
Data Retrievals	No additional cost*
<p><i>* Glacier is designed with the expectation that retrievals are infrequent and unusual, and data will be stored for extended periods of time. You can retrieve up to 5% of your average monthly storage (pro-rated daily) for free each month. If you choose to retrieve more than this amount of data in a month, you are charged a retrieval fee starting at \$0.011 per gigabyte. In addition, there is a pro-rated charge of \$0.032 per gigabyte for items deleted prior to 90 days.</i></p>	
<b>Storage Gateway</b>	
You are billed for the snapshots your gateway stores in Amazon S3. These snapshots are stored and billed as EBS snapshots.	
<b>Public Cloud Availability</b>	
Per activated gateway per month	2% off MSRP

## 1.10 Data Transfer

Data Transfer: Outbound, Inbound, Regional	
All Region Availability	Price Per GB
<b>Outbound</b>	
First GB per month	No additional cost
Up to 10 TB/Month	2% off MSRP
Next 40 TB/Month	2% off MSRP
Next 100 TB/Month	2% off MSRP
Next 350 TB/Month	2% off MSRP
<b>Inbound</b>	
Inbound GB/Month	No additional cost
<b>Regional</b>	
Regional data transfer in/out	2% off MSRP

## 1.11 All Other Cloud Services & Solutions

Compute Services	Cost Unit	Cost
EC2 Container Service (ECS)	Price per EC2 instances	2% off MSRP
AWS Lambda	Per 100 milliseconds	2% off MSRP
AWS Config	Price per configuration	2% off MSRP
AWS Mobile Hub		BETA
<b>VPN/VPC Services</b>		
Price Per VPN Connection Hour	Per Hour	2% off MSRP
Route 53		
<b>Hosted Zones</b>		
First 25 hosted zones	Price Per Hosted Zone Per Month	2% off MSRP

Compute Services	Cost Unit	Cost
Additional zones	Price Per Hosted Zone Per Month	2% off MSRP
<b>Standard Queries</b>		
First 1 Billion queries per month	Per Million Queries per Month	2% off MSRP
Over 1 Billion queries per month	Per Million Queries per Month	2% off MSRP
<b>Latency Based Routing Queries</b>		
First 1 Billion queries per month	Per Million Queries per Month	2% off MSRP
Over 1 Billion queries per month	Per Million Queries per Month	2% off MSRP
<b>Monitoring Services</b>		
Standard Monitoring	Price Per Month	No additional cost
Detailed Monitoring, Alerting, and Reporting	Price Per Month	2% off MSRP
Amazon CloudWatch Detailed Monitoring	Price per instance per month	2% off MSRP
Amazon CloudWatch Custom Metrics	Price per metric per month	2% off MSRP
Amazon CloudWatch Alarms/First 10 Alarms	Price per alarm per month	No additional cost
Amazon CloudWatch Alarms/After First 10 Alarms	Price per alarm per month	2% off MSRP
Amazon CloudWatch API Requests	Price per 1,000 Get, List, or Put requests	2% off MSRP
AWS CloudTrail		No additional cost
AWS Service Catalog	Price per Month	2% off MSRP
<b>IAM</b>		
IAM	Price Per User Per Month	No additional cost
<b>Provisioning Software</b>		
Provisioning Software	Fixed Price Per State Account Per Year	No additional cost
<b>Elastic Storage</b>		

Compute Services	Cost Unit	Cost
Elastic Block Storage	Price per GB per month	2% off MSRP
Elastic File System	Price per storage used	2% off MSRP
<b>Elastic Load Balancing</b>		
Elastic Load Balancing	Price per Hour	2% off MSRP
<b>Elastic Load Balancing Data Transfer</b>		
Elastic Load Balancing	Price per GB	2% off MSRP
<b>Snapshot Data Storage</b>		
Snapshot Data Storage	Price per GB per month	2% off MSRP
<b>Auto Scaling</b>		
Auto Scaling	Price per Hour	No additional cost
<b>EBS I/O Requests</b>		
I/O Requests	Price per 1 million	2% off MSRP
<b>Elastic IP Addresses</b>		
Elastic IP address associated (non-associated) with running instance	Price per Hour per month	2% off MSRP
Elastic IP address remap – first 100 remaps per month	Price per Month	No additional cost
Elastic IP address remap – additional remap per month over 100	Price per Month	2% off MSRP
<b>S3 Requests</b>		
PUT, COPY, POST, or LIST Requests	Per 1000 requests	2% off MSRP
GET and all other Requests	Per 10,000 requests	2% off MSRP
<b>Import/Export Tool</b>		
Storage Device	Per device	2% off MSRP
Data Loading Hour (Partial data-loading-hours are billed as full hours)	Price per Hour/Partial Hour	2% off MSRP
AWS Snowball (Up to 50 TB Snowball includes a high-speed, 10 Gbps network connection)		Call for Pricing

Compute Services	Cost Unit	Cost
AWS Data Pipeline	Price per Month	2% off MSRP
<b>SNS Requests/Notifications</b>		
SNS API Requests first 100,000	Price per Month	No additional cost
SNS API Requests after first 100,000	Price per Month	2% off MSRP
SNS HTTP/HTTPS Notifications first 100,000	Price per Month	No additional cost
SNS HTTP/HTTPS Notifications after first 100,000	Price per Month	2% off MSRP
SNS Email/Email-JSON Notifications first 1000	Price per Month	No additional cost
SNS Email/Email-JSON Notifications after first 1000	Price per 100,000 per Month	2% off MSRP
SNS SMS Notifications first 100	Price per Month	No additional cost
SNS SMS Notifications after first 100	Price per 100 per Month	2% off MSRP
<b>SQS</b>		
Price per 10,000 SQS Requests	Price per Month	2% off MSRP
<b>Encryption Services</b>		
AWS CloudHSM	Once per instance then hourly	2% off MSRP
AWS Key Management Service	Price per month per key	2% off MSRP
<b>Machine Learning</b>		
Amazon Machine Learning	Price per hour for compute time	2% off MSRP
<b>Code Services</b>		
AWS CodeDeploy	Price per instance	2% off MSRP
AWS Code Pipeline	Price per instance	2% off MSRP
AWS Code Commit	Price per user	2% off MSRP
Standard rates for Amazon S3 and Amazon SNS usage apply		
<b>Disaster Recovery/Migration Solutions (CloudEndure)</b>		
Product Description	Unit per Issue	Price



Compute Services		Cost Unit	Cost
Enterprise Disaster Recovery		Price per instance	\$99.00 (Annual Fee)
Enterprise Migration		Price per instance	\$299.00
Discovery (RISC Networks)			
Product Description	Unit per Issue	Price	
CloudScape (Standard)		Per Server/VM Monthly (0-500)	\$11.00
Enterprise Edition		Per Server/VM Monthly (501+)	\$7.50
Cisco InterCloud Fabric (Business)			
Cisco InterCloud Fabric (Business)		\$250 per VM (minimum – 2)	\$500.00

## 1.12 Infor SaaS Products

Infor understands and recognizes that each license opportunity is unique and extends prices based on the conditions of each individual opportunity. License pricing will be tailored and configured as a function of each individual opportunity.

Product Description	Unit Per Issue	Price
Landmark Technology Runtime Subscription	Employee	\$ -
Lawson System Foundation Subscription	Amazon EC2 Compute Unit	\$ 449.63
NetExpress App Runtime Subscription	Concurrent Users	\$ 719.40
Infor Notifications Subscription	Employee	\$ 1.44
Infor Process Automation Subscription	Employee	\$ 11.51
Infor Business Intelligence for Lawson - Subscription	CloudSuite Limited Use	\$ 503.58
Business Vault (Restricted Use) Subscription	CloudSuite Limited Use	\$ 1.44
BV Data Warehouse Designer Subscription (Restricted Use)	Employee	\$ 1.44
Infor Ming.le Enterprise Subscription	CloudSuite Limited Use	\$ 5.76
Infor ION PROCESS with Business Vault - Single Tenant - Subscription	CloudSuite Limited Use	\$ 7.19
Financial Procurement Subscription	Employee	\$ 30.21

Product Description	Unit Per Issue	Price
Mobile Projects Subscription	Employee	\$ 1.44
Mobile Assets Subscription	Employee	\$ 1.44
Mobile Financials Subscription	Employee	\$ 1.44
Infor Lawson Project Accounting Subscription	Employee	\$ 5.76
Lawson P2P Connectors Subscription	Employee	\$ 1.44
Lawson ION Connector Subscription	Employee	\$ 1.44
Procurement Punchout Subscription	Employee	\$ 5.76
Mobile Inventory Subscription	Employee	\$ 1.44
Mobile Requisitions Subscription	Employee	\$ 1.44
Procurement Card Self-Service Subscription	Employee	\$ 1.44
Requisition Center Subscription	Employee	\$ 21.58
Electronic Payment Connector Subscription	Employee	\$ 1.44
Smart Office Subscription	Employee	\$ 7.19
Addins For Microsoft Subscription	Employee	\$ 5.76
Implementation Accelerator for Public Sector ERP	Employee	\$ 1.44
Infor CloudSuite HCM Enterprise Product Suite Subscription	Employee	-
Landmark Technology Runtime Subscription 2	Employee	-
Infor Process Automation Subscription 2	Employee	8.19
ION Process iPaaS Platform - Multi-Tenant - Subscription	CloudSuite Limited Use	4,500.00
Infor Landmark Administrator Subscription	Employee	-
Infor Notifications Subscription 2	Employee	-
Addins For Microsoft Subscription 2	Employee	4.10
Infor Talent Manager Subscription	Employee	0.82
Global Human Resources Subscription	Employee	9.83
Talent Acquisition Subscription	Employee	9.01

Product Description	Unit Per Issue	Price
Compensation Management Subscription	Employee	9.01
Goal Management Subscription	Employee	9.01
Performance Management Subscription	Employee	9.01
Succession Management Subscription	Employee	9.01
Development Planning Subscription	Employee	9.01
Infor Mobile Recruiter Subscription	Employee	0.74
Talent Mgmt Lang Pack US Eng (en-US) Subscription	Enterprise	696.15
Talent Mgmt Lang Pack UK Eng (en-GB) Subscription	Enterprise	696.15
Talent Mgmt Lang Pack French (fr) Subscription	Enterprise	696.15
Talent Mgmt Lang Pack French Canadian (fr-CA) Subscription	Enterprise	696.15
Talent Mgmt Lang Pack German (de) Subscription	Enterprise	696.15
Talent Mgmt Lang Pack Spanish (es) Subscription	Enterprise	696.15
Talent Science Predictive Talent Analytics Assessment Subscription	Employee	46.80
Talent Science Advanced Reporting Subscription	Enterprise	-
Talent Science Standard Workflow Management Subscription	Enterprise	-
Talent Science Custom Performance Profiles Subscription	CloudSuite Limited Use	-
Talent Science Best Practice Profiles Subscription	CloudSuite Limited Use	-
Talent Science Strategic Leadership Insights Subscription	Employee	-
Single Sign On Subscription	Enterprise	1,170.00
Knowledgebase Subscription	Employee	8.19
Knowledgebase Benefit Decision Support Subscription	Employee	3.51
Case Management Subscription	Employee	7.02
Mobile HR Service Delivery Subscription	Employee	-
Knowledgebase/Case Management French (France) Translation Subscription	Enterprise	468.00
Knowledgebase/Case Management Canadian French Translation Subscription	Enterprise	468.00

Product Description	Unit Per Issue	Price
Knowledgebase/Case Management German Translation Subscription	Enterprise	468.00
Knowledgebase/Case Management Spanish (Spain) Translation Subscription	Enterprise	468.00
Knowledgebase/Case Management Mexican Spanish Translation Subscription	Enterprise	468.00
Knowledgebase Non US Implementations Subscription	Employee	1.17
Learning Management Subscription	Employee	9.36
Learning Management Content Management Subscription	Employee	5.85
Learning Management Content Creation Developer License Subscription	Named Users	-
Learning Management Ad-Hoc Reporting Subscription	Employee	2.34
Learning Management Advanced Certification and Compliance Subscription	Employee	2.34
Learning Management Mobile Learning Subscription	Employee	1.17
Learning Management: Inactive Users Subscription	Employee	1.17
Learning Management Language Pack: Portal Only English - UK (en-gb) Subscription	Enterprise	234.00
Learning Management Language Pack: French (fr) Subscription	Enterprise	234.00
Learning Management Language Pack: Portal Only French - Canada (fr-ca) Subscription	Enterprise	234.00
Learning Management Language Pack: German (de) Subscription	Enterprise	234.00
Learning Management Language Pack: Spanish (es-es) Subscription	Enterprise	234.00
Hansen 8 - Asset Management Bundle Subscription	Named Users	-
Hansen 8 - Asset Management for Facilities Subscription	Named Users	360.00
Hansen 8 - Asset Management for Transportation Subscription	Named Users	360.00
Hansen 8 - Asset Management for Utilities Subscription	Named Users	360.00
Hansen 8 - Configured Assets Subscription	Named Users	72.00
Hansen 8 - CDR Web Services Subscription	Named Users	72.00
Hansen 8 - Assets Web Services Subscription	Named Users	72.00
Hansen 8 - Billing Web Services Subscription	Named Users	72.00
Hansen 8 - Work Management Subscription	Named Users	72.00

Product Description	Unit Per Issue	Price
Hansen 8 - Customer Service Subscription	Named Users	72.00
Hansen 8 - Open 311 API Subscription	Named Users	72.00
Hansen 8 - Microsoft Exchange Subscription	Named Users	72.00
Hansen 8 - Asset Valuation Subscription	Named Users	144.00
Hansen 8 - CDR Enhanced Bundle Subscription	Named Users	-
Hansen 8 - CDR Bundle Subscription	Named Users	882.00
Hansen 8 - Open 311 API Subscription 2	Named Users	75.60
Hansen 8 - Microsoft Exchange Subscription 2	Named Users	75.60
Hansen 8 - CDR Web Services Subscription 2	Named Users	75.60
Hansen 8 - Assets Web Services Subscription 2	Named Users	75.60
Hansen 8 - Billing Web Services Subscription 2	Named Users	75.60
Hansen 8 - Customer Service Bundle Subscription	Named Users	-
Hansen 8 - Customer Service Subscription 2	Named Users	504.00
Hansen 8 - Call Center Subscription	Named Users	72.00
Hansen 8 - Open 311 API Subscription 3	Named Users	28.80
Hansen 8 - Microsoft Exchange Subscription 3	Named Users	28.80
Hansen 8 - CDR Web Services Subscription 3	Named Users	28.80
Hansen 8 - Assets Web Services Subscription 3	Named Users	28.80
Hansen 8 - Billing Web Services Subscription 3	Named Users	28.80
Hansen 8 - Life Cycle Analysis and Risk Bundle Subscription	Named Users	-
Hansen 8 - Life Cycle Analysis Subscription	Named Users	450.00
Hansen 8 - Risk Subscription	Named Users	450.00
Hansen 8 - Advanced Assets Bundle Subscription	Named Users	900.00
Hansen 8 - Asset Analysis Subscription	Named Users	450.00
Hansen 8 - Asset Management Tools Subscription	Named Users	450.00

Product Description	Unit Per Issue	Price
Hansen Dynamic Portal for CDR Subscription	Population	-
Hansen Dynamic Portal for Permits Subscription	Population	0.12
Hansen Dynamic Portal for Licensing Subscription	Population	0.12
Hansen Dynamic Portal for Planning Subscription	Population	0.12
Hansen Dynamic Portal - Use Module Subscription	Population	0.12
Hansen Dynamic Portal for Customer Service - Responsive Design Subscription	Population	0.12
Hansen 8 - Utility Billing Bundle Subscription	Accounts	-
Hansen 8 - CIS Billing Subscription	Accounts	1.92
Hansen 8 - Open 311 API Subscription 4	Named Users	0.10
Hansen 8 - Microsoft Exchange Subscription 4	Named Users	0.10
Hansen 8 - CDR Web Services Subscription 4	Named Users	0.10
Hansen 8 - Assets Web Services Subscription 4	Named Users	0.10
Hansen 8 - Billing Web Services Subscription 4	Named Users	0.10
Dynamic Portal for Customer Service - Responsive Design Subscription2	Population	0.30
Dynamic Portal for Utility Billing Responsive Design Subscription	Accounts	0.24
Infor Field Inspector Work Management Subscription	Named Users	300.00
Hansen - Water Meter Management Subscription	Named Users	450.00
Hansen 8 - Solid Waste Container Management Subscription	Named Users	450.00
Hansen 8 - CDR Billing Subscription	Annual Transactions	2.40
Hansen 8 - Work Management Subscription 2	Named Users	900.00
Hansen 8 Cashiering Subscription	Named Users	1,200.00
Infor Field Inspector CDR Subscription	Named Users	300.00
Infor CRM Enterprise Subscription	Named Users	780.00
Infor CRM Enterprise Subscription 2	Concurrent Users	1,200.00
Infor CRM Architect Subscription	Named Users	-

Product Description	Unit Per Issue	Price
Infor CRM SaaS Storage Subscription	1.0GB	-
Crystal Reports Designer Subscription	Named Users	-
Infor CRM Enterprise Web Viewer Subscription	Named Users	240.00
Infor CRM Enterprise Mobile Only Subscription	Named Users	300.00
Infor CRM Enterprise Subscription 3	Named Users	600.00
Infor CRM Enterprise Subscription 4	Concurrent Users	900.00
Infor CRM Architect Subscription 2	Named Users	-
Infor CRM SaaS Storage Subscription 2	1.0GB	-
Crystal Reports Designer Subscription 2	Named Users	-
Infor CRM Enterprise Web Viewer Subscription 2	Named Users	180.00
Infor CRM Enterprise Mobile Only Subscription 2	Named Users	300.00
Infor CRM Professional Subscription	Named Users	420.00
Infor CRM SaaS Storage Subscription 3	1.0GB	-
Crystal Reports Designer Subscription 3	Named Users	-
Infor CRM Sync for Exchange Subscription	Named Users	120.00
Infor CRM Sync for Gmail Subscription	Named Users	120.00
Infor CRM Cloud Bridge	Virtual Private Network	7,320.00
Infor CRM Managed Server Tier 1 Subscription	Server	1,560.00
Infor CRM Managed Server Tier 2 Subscription	Server	3,120.00
Infor CRM Managed Server Tier 3 Subscription	Server	4,680.00
Infor CRM SaaS Storage Subscription 4	1.0GB	30.00
Infor CRM Adv SpeedSearch Unltd Subscription	Enterprise	1,188.00
Infor CRM Offline Web Client Subscription	Named Users	240.00
Infor CRM Limited use Named user for Lead Capture Subscription	Named Users	420.00
Infor CRM Adv Analytics Standard Subscription	Named Users	180.00

Product Description	Unit Per Issue	Price
Infor CRM Adv Analytics Pro Subscription	Named Users	720.00
Infor CRM Self Service Portal Limited Subscription	Concurrent Users	42.00
Infor CRM Staging: Secured Environment Subscription	Sandbox Instance Days	20.00
Infor CRM KS Corporate Edition Tier 1 Subscription	Server	2,760.00
Infor CRM KS Corporate Edition Tier 2 Subscription	Server	5,520.00
Infor CRM KS Corporate Edition Tier 3 Subscription	Server	8,280.00
Infor CRM KS Enterprise Edition Tier 1 Subscription	Server	3,120.00
Infor CRM KS Enterprise Edition Tier 2 Subscription	Server	6,240.00
Infor CRM KS Enterprise Edition Tier 3 Subscription	Server	9,360.00
Infor CRM KS Connector for Infor CRM Subscription	Application Connection	-
Infor CRM KS Connector for Email Server Subscription	Application Connection	-
Infor CRM Salesfusion Core Package Subscription	Sending Domains	5,700.00
Infor CRM Salesfusion Contacts Subscription	Email Contacts	-
Infor CRM Salesfusion Performance Pack Subscription	Sending Domains	1,400.00
Infor CRM Salesfusion CRM Integration Fee Subscription	Enterprise	600.00
Infor CRM Salesfusion Contacts Subscription 2	Email Contacts	0.12
Infor CRM Salesfusion Dedicated IP Subscription	IP Address	3,000.00
Infor CRM Salesfusion Sandbox Subscription	Enterprise	1,200.00
Infor CRM Salesfusion Quick Start Service Subscription	Each	11,940.00
Infor CRM Salesfusion Onboarding Service	Each	995.00
Infor CRM Salesfusion Onboarding Service 2	Each	-
EMS Interaction Advisor Server Professional for the Cloud	CPU Cores	23,970.00
EMS Interaction Advisor Manager for the Cloud	Named Users	468.00
EMS Interaction Advisor for Salesforce	Named Users	300.00
Inforce for Salesforce	Named Users	360.00



Product Description	Unit Per Issue	Price
Infor ION CONNECT for Inforce - Subscription	Named Users	120.00
Additional Contacts for LG Email Bundles	Million Units	2,000.00
SFDC Sales Cloud (Enterprise Edition)	Named Users	1,500.00
SFDC Service Cloud (Enterprise Edition)	Named Users	1,620.00
SFDC Mobile	Named Users	600.00
SFDC API Calls - 10,000 additional calls per day per license	API10K	300.00
SFDC Knowledge	Named Users	600.00
SFDC Service Cloud Portal	Named Users	6.75
SFDC Configuration-only Sandbox	Enterprise	156.00
SFDC Data Storage 500mb	0.5GB	900.00
SFDC File Storage 1G	1.0GB	120.00
SFDC File Storage 10G	10GB	960.00
SFDC Full Sandbox for testing	Enterprise	624.00
Talent Science Predictive Talent Analytics Assessment Subscription 2	Employee in Scope	51.00
Talent Science Advanced Reporting Subscription 2	Enterprise	-
Talent Science Standard Workflow Management Subscription 2	Enterprise	-
Talent Science Custom Performance Profiles Subscription 2	Unique Profile	3,300.00
Talent Science Training Credits / Subscription	Training Credits	120.00
Talent Science Applicant Tracking System (ATS) Subscription	Enterprise	3,326.40
Talent Science Custom Workflow Management Subscription	Unique Workflow	-
Talent Science Career Portal Subscription	Web Portal	-
Talent Science Employment Application Subscription	Web Form	-
Talent Science ATS Requisition Management Subscription	Enterprise	4,104.00
Talent Science Custom Workflow Management Subscription 2	Unique Workflow	2,400.00
Talent Science Advanced Key Word Search Subscription	Enterprise	5,100.00

Product Description	Unit Per Issue	Price
Talent Science Career Portal Subscription 2	Web Portal	1,200.00
Talent Science Employment Application Subscription 2	Web Form	2,400.00
Talent Science Custom Strategic Leadership Insights Job Template Subscription	Unique Template	1,500.00
Talent Science - Candidate Retention Subscription	Retention Years	12,000.00
Talent Science Candidate Data Export (CDX) Subscription	Scheduled Export/Import	Data 5,000.00
Talent Science Business Edition Subscription	Employee	30.00
Talent Science ATS Requisition Management Subscription 2	Enterprise	18.00
Talent Science Advanced Key Word Search Subscription 2	Enterprise	12.00
Talent Science Integrations - ATS Healthcare Source Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS HR Logix Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS HR Smart Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS ICIMS Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Jobpartners Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Kenexa Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Kronos Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Oracle Subscription	Enterprise	9,600.00
Talent Science Integrations - ATS PC Recruiter Subscription	Enterprise	14,160.00
Talent Science Integrations - HRNX Setup Fee (1 time / customer)	Each	5,000.00
Talent Science Integrations - ATS PeopleFluent Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS PeopleSoft Subscription	Enterprise	9,600.00
Talent Science Integrations - ATS Pereless Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Position Manager Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Silk Road Subscription	Enterprise	14,160.00
Talent Science Integrations - HRNX Setup Fee (1 time / customer) 2	Each	5,000.00
Talent Science Integrations - ATS SnapHire Subscription	Enterprise	6,000.00

Product Description	Unit Per Issue	Price
Talent Science Integrations - ATS SuccessFactors Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Taleo Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS TechnoMedia Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS The Right Thing Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Ultimate Subscription	Enterprise	6,000.00
Talent Science Integrations - ATS Virtual Edge Subscription	Enterprise	6,000.00
Talent Science Integrations - Background Check ADP SASS Subscription	Enterprise	9,600.00
Talent Science Integrations - Background Check ESS (Deverus) Subscription	Enterprise	18,000.00
Talent Science Integrations - Background Check GIS Subscription	Enterprise	6,000.00
Talent Science Integrations - Background Check Group One Subscription	Enterprise	18,000.00
Talent Science Integrations - Background Check Hire Right Subscription	Enterprise	18,000.00
Talent Science Integrations - Background Check LexisNexis/Choice Point Subscription	Enterprise	6,000.00
Talent Science Integrations - Background Check Liberty Subscription	Enterprise	18,000.00
Talent Science Integrations - Background Check Moore (Deverus) Subscription	Enterprise	18,000.00
Talent Science Integrations - Background Check Quest Subscription	Enterprise	26,160.00
Talent Science Integrations - Background Check Safer Places Subscription	Enterprise	6,000.00
Talent Science Integrations - Background Check Sterling Subscription	Enterprise	6,000.00
Talent Science Integrations - Background Check TalentWise Subscription	Enterprise	6,000.00
Talent Science Integrations - Background Check TransUnion Subscription	Enterprise	9,600.00
Talent Science Integrations - Background Check Vereda Subscription	Enterprise	18,000.00
Talent Science Integrations - Job Board CareerBuilder Subscription	Enterprise	6,000.00
Talent Science Integrations - Job Board Hcareers Subscription	Enterprise	9,600.00
Talent Science Integrations - Job Board Monster Subscription	Enterprise	6,000.00
Talent Science Integrations - New ATS Subscription	Enterprise	18,000.00
Talent Science Integrations - New Background Check Subscription	Enterprise	26,400.00

Product Description	Unit Per Issue	Price
Talent Science Integrations - New Document Storage Subscription	Enterprise	26,400.00
Talent Science Integrations - New Job Board Subscription	Enterprise	18,000.00
Talent Science Integrations - New LMS Subscription	Enterprise	26,400.00
Talent Science Integrations - New Location Synchronization Subscription	Enterprise	9,600.00
Talent Science Integrations - New Onboarding Paperwork Subscription	Enterprise	26,400.00
Talent Science Integrations - New PeopleAnswers Format SSO Subscription	Enterprise	6,000.00
Talent Science Integrations - New Performance Management Subscription	Enterprise	26,400.00
Talent Science Integrations - New Rehire Eligibility Subscription	Enterprise	26,400.00
Talent Science Integrations - New Requisition Creation Subscription	Enterprise	26,400.00
Talent Science Integrations - New SAML SSO Subscription	Enterprise	18,000.00
Talent Science Integrations - New Skills Test Subscription	Enterprise	18,000.00
Talent Science Integrations - New User Synchronization Subscription	Enterprise	9,600.00
Talent Science Integrations - New Wage Verification Subscription	Enterprise	26,400.00
Talent Science Integrations - New Web Service HRIS Subscription	Enterprise	26,400.00
Talent Science Integrations - New WOTC Subscription	Enterprise	26,400.00
Talent Science Integrations - Onboarding ExponentHR Subscription	Enterprise	6,000.00
Talent Science Integrations - Onboarding KMS Subscription	Enterprise	18,000.00
Talent Science Integrations - Onboarding Silk Road Red Carpet Subscription	Enterprise	9,600.00
Talent Science Integrations - Onboarding TalentWise Subscription	Enterprise	9,600.00
Talent Science Integrations - Onboarding TALX Subscription	Enterprise	9,600.00
Talent Science Integrations - Onboarding USVerify Subscription	Enterprise	9,600.00
Talent Science Integrations - Rehire Eligibility ExponentHR Subscription	Enterprise	6,000.00
Talent Science Integrations - Skill Testing Performance Associates Subscription	Enterprise	18,000.00
Talent Science Integrations - Skill Testing PreVisor Subscription	Enterprise	18,000.00
Talent Science Integrations - Web Service HRIS ADP Subscription	Enterprise	9,600.00

Product Description	Unit Per Issue	Price
Talent Science Integrations - Web Service HRIS Workday Subscription	Enterprise	9,600.00
Talent Science Integrations - WOTC ADP Subscription	Enterprise	6,000.00
Talent Science Integrations - WOTC Ernst & Young Subscription	Enterprise	6,000.00
Talent Science Integrations - WOTC Maximus Subscription	Enterprise	6,000.00
Talent Science Integrations - WOTC TALX Subscription	Enterprise	6,000.00
Talent Science Integrations - WOTC TaxBreak Subscription	Enterprise	6,000.00
TalentWise e-Portal Custom Branding Subscription	Site	75.00
TalentWise e-Portal Custom Branding Subscription - One-time Setup	Site	1,000.00
TalentWise e-Portal Form Storage Subscription	Site	375.00
TalentWise e-Portal Form Storage Subscription - One-time Setup	Site	1,000.00
TalentWise e-Wage - CA Theft Prevention Act Subscription	Site	105.00
TalentWise e-Wage - CA Theft Prevention Act Subscription - One-time Setup	Site	250.00
TalentWise e-Wage - NY Theft Prevention Act Subscription	Site	105.00
TalentWise e-Wage - NY Theft Prevention Act Subscription - One-time Setup	Site	250.00
TalentWise e-Wage - PA Residency Act Subscription	Site	105.00
TalentWise e-Wage - PA Residency Act Subscription - One-time Setup	Site	250.00
TalentWise Payroll Data Export Subscription	Site	375.00
TalentWise Payroll Data Export Subscription - One-time Setup	Site	300.00
TalentWise Standard Data Export Subscription	Site	300.00
TalentWise Standard Data Export Subscription - One-time Setup	Site	750.00
TalentWise New Hire Forms - Electronic Direct Deposit Subscription	Site	150.00
TalentWise New Hire Forms - Electronic Direct Deposit Subscription - One-time Setup	Site	500.00
TalentWise New Hire Forms - Emergency Contact Subscription	Site	150.00
TalentWise New Hire Forms - Emergency Contact Subscription - One-time Setup	Site	500.00
TalentWise New Hire Forms - New Employee EEO Subscription	Site	150.00

Product Description	Unit Per Issue	Price
TalentWise New Hire Forms - New Employee EEO Subscription - One-time Setup	Site	500.00
TalentWise New Hire Forms - Pay Card Acknowledgement Subscription	Site	150.00
TalentWise New Hire Forms - Pay Card Acknowledgement Subscription - One-time Setup	Site	500.00
TalentWise New Hire Forms - Policy Acknowledgement Subscription	Site	150.00
TalentWise New Hire Forms - Policy Acknowledgement Subscription - One-time Setup	Site	500.00
TalentWise New Hire Forms - New Employee Summary Subscription	Site	150.00
TalentWise New Hire Forms - New Employee Summary Subscription - One-time Setup	Site	500.00
TalentWise New Hire Forms - Uniform Order and Policy Acknowledgement Subscription	Site	150.00
TalentWise New Hire Forms - Uniform Order and Policy Acknowledgement Subscription - One-time Setup	Site	500.00
TalentWise Wage Mangement (Federal I9 and W4) Subscription	Site	105.00
TalentWise Wage Mangement (Federal I9 and W4) Subscription - One-time Setup	Site	250.00
Infor CloudSuite Facilities Management Professional User	Named Users	-
Infor EAM Enterprise Edition Subscription	Named Users	195.00
Infor EAM Enterprise Edition Customer Service Request Subscription	Named Users	105.00
Infor EAM Enterprise Edition Advanced Reporting Consumer Subscription	Named Users	105.00
Infor EAM Enterprise Edition Advanced Reporting Author Subscription	Named Users	105.00
Infor EAM Enterprise Edition Barcoding Subscription	Named Users	105.00
Infor EAM Enterprise Edition Databridge Subscription	Data Center	1,050.00
Infor EAM Enterprise Edition Mobile Subscription	Device	105.00
Infor EAM Enterprise Edition Requestor Subscription	Named Users	105.00
Infor EAM Alert Management Subscription	Data Center	1,050.00
Infor EAM Enterprise Edition Web Services Connector Subscription	Connector User	105.00
Infor EAM Enterprise Edition Web Services Toolkit Subscription	Data Center	1,050.00

Product Description	Unit Per Issue	Price
Infor EAM Asset Sustainability	Data Center	1,050.00
Infor Ming.le Enterprise User Subscription (Cloud Edition)	Named Users	75.00
ION Process iPaaS Platform - Multi-Tenant - Subscription 2	CloudSuite Limited Use	75.00
Infor CloudSuite Facilities Management Casual User	Named Users	-
Infor EAM Enterprise Edition Customer Service Request Subscription 2	Named Users	6.00
Infor EAM Enterprise Edition Requestor Subscription 2	Named Users	6.00
Infor EAM Enterprise Edition Web Services Connector Subscription 2	Connector User	6.00
Infor EAM Enterprise Edition Web Services Toolkit Subscription 2	Data Center	60.00
Infor EAM Enterprise Edition Subscription 2	Named Users	1,498.00
Infor EAM Enterprise Edition Requestor Subscription 3	Named Users	84.00
Infor EAM Energy Performance Management Module Subscription	Data Center	20,916.00
Infor EAM Energy Performance Management Module Device Subscription	Device	288.00
Infor EAM Asset Sustainability 2	Data Center	13,944.00
Infor EAM Asset Sustainability Device	Device	288.00
Infor EAM Alert Management Subscription 2	Data Center	13,944.00
Infor Energy Performance Management Edition	Named Users	3,500.00
Infor EAM Enterprise Edition GIS Subscription	Data Center	13,944.00
Infor EAM Enterprise Edition Web Services Toolkit Subscription 3	Data Center	13,944.00
Infor EAM Enterprise Edition Web Services Connector Subscription 3	Connector User	1,332.00
Infor EAM Enterprise Edition Advanced Reporting Consumer Subscription 2	Named Users	-
Infor EAM Enterprise Edition Advanced Reporting Author Subscription 2	Named Users	-
Infor EAM Enterprise Edition Calibration Subscription	Data Center	13,944.00
Infor EAM Enterprise Edition Electronic Record / Signature Subscription	Data Center	13,944.00
Infor EAM Enterprise Edition Fleet Management Subscription	Data Center	13,944.00
Infor EAM Enterprise Edition Databridge Subscription 2	Data Center	13,944.00

Product Description	Unit Per Issue	Price
Infor EAM Enterprise Edition Databridge Subscription - Application Specific	Data Center	-
Infor EAM Enterprise Edition Mobile Subscription 2	Device	1,020.00
Infor EAM Enterprise Edition Barcoding Subscription 2	Named Users	288.00
Infor EAM Enterprise Edition Customer Service Request Subscription 3	Named Users	0.29
Infor EAM Enterprise Edition Advanced Maintenance Planning Subscription	Data Center	13,944.00
Infor EAM Enterprise Edition Advanced Maintenance Planning Subscription - Application Specific	Data Center	-
Infor EAM Enterprise Edition Reliability Planning and Analysis Subscription	Data Center	13,944.00
Implementation Accelerator for EAM Industrial Manufacturing - Subscription	Enterprise	3,914.16
Infor10 EAM Enterprise Sustainability – ENXSuite	Named Users	3,000.00
Infor EAM Asset Sustainability Edition Subscription	Named Users	1,308.00
Infor EAM Asset Sustainability Edition Metered Asset Subscription Device	Device	288.00
Infor EAM Asset Sustainability Edition Metered Asset Subscription	Data Center	8,400.00
Infor EAM Asset Sustainability Edition Requestor Subscription	Named Users	84.00
Infor EAM Asset Sustainability Edition GIS Subscription	Data Center	8,400.00
Infor EAM Asset Sustainability Edition Web Services Toolkit Subscription	Data Center	8,400.00
Infor EAM Asset Sustainability Edition Web Services Connector Subscription	Connector User	1,332.00
Infor EAM Asset Sustainability Edition Advanced Reporting Consumer Subscription	Named Users	-
Infor EAM Asset Sustainability Edition Advanced Reporting Author Subscription	Named Users	-
Infor EAM Asset Sustainability Edition Calibration Subscription	Data Center	9,780.00
Infor EAM Asset Sustainability Edition Electronic Record / Signature Subscription	Data Center	6,960.00
Infor EAM Asset Sustainability Edition Fleet Management Subscription	Data Center	5,580.00
Infor EAM Asset Sustainability Edition Databridge Subscription	Data Center	9,780.00
Infor EAM Asset Sustainability Edition Databridge Subscription - Application Specific	Data Center	-
Infor EAM Asset Sustainability Edition Mobile Subscription	Device	1,020.00



Product Description	Unit Per Issue	Price
Infor EAM Asset Sustainability Edition Barcoding Subscription	Named Users	288.00
Infor EAM Asset Sustainability Edition Customer Service Request Subscription	Named Users	0.29
Infor EAM Asset Sustainability Edition Advanced Maintenance Planning Subscription	Data Center	13,980.00
Infor EAM Asset Sustainability Edition Advanced Maintenance Planning Subscription - Application Spec	Data Center	-
Infor d/EPM Subscription	Named Users	3,600.00
Infor BI Subscription	Named Users	2,100.00
Infor BI Dashboards (app) Subscription	Named Users	240.00
Workforce Platform - Employee Transaction Manager Subscription	End User	4.56
Workforce Platform - Workmail/Form Builder/Workflow Editor	End User	6.00
Workforce Planning - Budget Management & Creation	End User	23.40
Workforce Relief Management Subscription	End User	12.00
Workforce Scheduling - Labor Forecasting & Schedule Optimization	End User	36.00
Workforce Task Management Subscription	Site	1,200.00
Workforce Scheduling - Schedule Bidding	End User	27.00
Workforce Scheduling - Labor Scheduler	End User	34.20
Workforce Scheduling - Shift Trading	End User	11.28
Workforce Time & Attendance - Time & Attendance Subscription	End User	45.00
Workforce Absence - Attendance Management	End User	7.20
Workforce Language Pack - Chinese Simplified	End User	0.60
Workforce Language Pack - Chinese Traditional	End User	0.60
Workforce Language Pack - Czech	End User	0.60
Workforce Language Pack - Dutch	End User	0.60
Workforce Language Pack - Finnish	End User	0.60
Workforce Language Pack - French (Canadian)	End User	0.60
Workforce Language Pack - French (European)	End User	0.60

Product Description	Unit Per Issue	Price
Workforce Language Pack - German	End User	0.60
Workforce Language Pack - Hungarian	End User	0.60
Workforce Language Pack - Italian	End User	0.60
Workforce Language Pack - Korean	End User	0.60
Workforce Language Pack - Polish	End User	0.60
Workforce Language Pack - Portuguese (Brazilian)	End User	0.60
Workforce Language Pack - Russian	End User	0.60
Workforce Language Pack - Spanish (European)	End User	0.60
Workforce Language Pack - Spanish (Latin American)	End User	0.60
Workforce Language Pack - Turkish	End User	0.60
EPAK Developer Seat - Workforce Subscription	EPAK Named User	60,000.00
EPAK Content - Workforce - Time and Attendance Subscription	EPAK Named User	0.60
EPAK Content - Workforce - Labor Forecasting Scheduling Optimization Subscription	EPAK Named User	0.60
EPAK Content - Workforce - Multi-view Scheduler Subscription	EPAK Named User	0.60
EPAK Content - Workforce - Real-time Self Scheduler Subscription	EPAK Named User	0.60
EPAK Content - Workforce - Employee Transaction Manager Subscription	EPAK Named User	0.60
Workforce Mobility - Mobile Shift Scheduler Subscription	Employee	12.00
Infor ION PROCESS with Business Vault - Single Tenant - Subscription 2	Virtual Core	51,600.00
ION Process iPaaS Platform - Multi-Tenant - Subscription 3	Virtual Core	19,200.00
ION Process iPaaS Hybrid Connector - Multi-Tenant - Subscription	Location	6,000.00
Infor ION Connector for SAP - SaaS Single Tenant	Virtual Core	43,200.00
Infor ION Connector for Oracle EBS - SaaS Single Tenant	Virtual Core	43,200.00
Infor Ming.le Enterprise Subscription 2	Named Users	408.00
Infor Ming.le Enterprise User Subscription (Cloud Edition) 2	Named Users	108.00
Infor Ming.le Basic User Subscription (Cloud Edition)	Named Users	48.00

Product Description	Unit Per Issue	Price
Infor Ming.le External User Subscription (Cloud Edition)	Named Users	18.00
Infor Document Management Subscription Single Tenant	Named Users	432.00
Infor Document Management - Document Capture Subscription Single Tenant	Annual Images	0.32
Expense Management Subscription for Expense Reports	Named Users	11,000.00
Expense Management Subscription for Payment Request	Documents	3,000.00
Expense Management Subscription for Payment Request 2	Named Users	11,000.00
Expense Management Subscription for Travel Plans	Named Users	5,500.00
Expense Management Subscription for Time Sheets	Named Users	5,500.00
Infor Reporting for Expense Management Subscription	Named Users	172.08
Infor Reporting - Consumer Subscription	Named Users	148.80
Infor Reporting - Analytics User Subscription	Named Users	82.80
Infor Reporting - Web Admin Subscription	Named Users	112.80
Infor Ming.le Basic User Subscription (Cloud Edition) 2	Named Users	120.00
SaaS Subscription - Cognos BI Consumer Pack with Author License	Cognos Pack X5	9,600.00

*\* SaaS Terms are Renewed at 6% uplifts*

*\* Annual Pricing*

*\*Products with no line item pricing are administrative line items for provisioning license rights.*

## 1.13 Data Analytics

Day1 provides a robust suite of capabilities to address your data analytics, business intelligence and visualization needs in order to help facilitate the process of data driven decision-making. Data Analytics as a Service (DAaaS) gives government agencies the ability to leverage our deep expertise of Amazon Web Services (AWS) Big Data and Analytics (BDA) suite with a Bring Your Own License (BYOL) model. Pricing below includes the ingestion, processing and output of intelligence based on the amount of data being analyzed.

Day1-Data Analytics as a Service (DAaaS)	Data Size Limit	Unit Price
Structured Data	≤250GB	\$5,000

Day1-Data Analytics as a Service (DAaaS)	Data Size Limit	Unit Price
Unstructured Data	≤100GB	\$10,000

### 1.14 Maintenance and Support

Day1’s Managed Services offering provides a tailored holistic approach environment support; we develop a relationship with your team and maintain your cloud architecture allowing you to focus on using it. We currently support 3 tiers of service level that will serve as a baseline for your cloud compute environment. Our Bronze, Silver and Gold packages deliver a granularity to investment with Day1, we can approach an environment providing only the most critical support to notify customers of an emergency situation and while adhering to SLAs we allow the customer to utilize our remediation services at an additional hourly rate. This empowers our customer to leverage in house resources for what makes sense and to only use us where necessary. Our Silver offering is where most of our customers feel most comfortable. This tier includes 24x7x365 response on top of our monitoring and notification. We will be available at any time to quickly troubleshoot the incident and keep the customer informed as we remediate the problem. We also support more of the relationship to the cloud environment, by providing operational maintenance to keep things running efficiently. We will support all standard patching and updates, on-demand machine and drive imaging and resizing as well as, DR & Backup Validation. We also support Infrastructure cost review, security review, and customer dashboards to allow a deeper level of collaboration with our service. Our Gold level offering is for customers looking to utilize Day1 as an advisor and support highly available services and environments. All Silver level support is included and hardened to support the increased complexity of the environment. We also will handle Code Release Support, to ensure rapid deployment of features or updates will not compromise the environment. The security review and backup/DR processes become more granular and will include human intervention on top of a strong automated approach. Day1 will work with your team to provide highly customized dashboards to reflect the individual metrics your company needs to measure success, on top of the critical health metrics. We continually and proactively monitor your system to track key metrics, maintain maximum uptime, and provide notification should issues arise. Managed Services is ideal for clients wishing to take advantage of the cost savings and flexibility of a cloud environment without taking on the daily operations and management that come with it. Pricing for Managed Services may vary and is based on the complexity of the cloud environment including architecture, number of servers, operating system, software, and usage.

Maintenance & Support	
Support	Monthly Price
Bronze	Standard AWS Compute Instance: \$75.00 Standard AWS RDS Instance: \$150.00 Elastic Load Balancer: \$37.50
Silver	Standard AWS Compute Instance: \$150.00 Standard AWS RDS Instance: \$225.00 Elastic Load Balancer: \$37.50
Gold	Standard AWS Compute Instance: \$225.00 Standard AWS RDS Instance: \$300.00 Elastic Load Balancer: \$37.50

Maintenance & Support	
Optional Service Add-Ons	Standard Priority Service Rate: \$150.00 / Hour Priority Service Rate: \$175.00 / Hour Rush Service Rate: \$225.00 / Hour
AWS Business Support (Required)	MSRP
AWS Enterprise Support (Optional)	MSRP

Professional and Consulting services can be added to any of our support plans to cover additional services such as migration planning, readiness assessment, system design and architecture, system provisioning or de-provisioning, deployment, development and testing, and security assessments.

### 1.15 Professional & Consulting Services

Day1 Consulting Services (onsite/offsite)	Price Per Hour
<b>Generalists</b>	
IT Professional 1	\$ 74.42
IT Professional 2	\$ 96.75
IT Professional 3	\$ 112.29
Business Process Engineer 1	\$ 83.16
Business Process Engineer 2	\$ 102.46
Business Process Engineer 3	\$ 120.78
Functional Analyst 1	\$ 90.15
Functional Analyst 2	\$ 112.45
Functional Analyst 3	\$ 138.60
<b>Consultants</b>	
Consulting Engineer 1	\$ 129.75
Consulting Engineer 2	\$ 142.69
Consulting Engineer 3	\$ 169.14
DevOps Engineer 1	\$ 144.97

Day1 Consulting Services (onsite/offsite)	Price Per Hour
DevOps Engineer 2	\$ 183.36
DevOps Engineer 3	\$ 199.86
Big Data Scientist 1	\$ 144.97
Big Data Scientist 2	\$ 183.36
Big Data Scientist 3	\$ 199.86
Solutions Architect 1	\$ 181.21
Solutions Architect 2	\$ 229.20
Solutions Architect 3	\$ 249.82
Principal Solutions Architect	\$ 287.29
<b>Performance Management</b>	
Project Manager 1	\$ 110.83
Project Manager 2	\$ 136.13
Program Manager	\$ 158.28
<b>Technical Specialists</b>	
Subject Matter Expert 1	\$ 142.62
Subject Matter Expert 2	\$ 165.24
Subject Matter Expert 3	\$ 203.31
Database Management Specialist 1	\$ 145.20
Database Management Specialist 2	\$ 168.20
Database Management Specialist 2	\$ 182.71
Training Specialists 1	\$ 142.62
Training Specialists 2	\$ 165.24
Training Specialists 3	\$ 203.31

## 1.16 Other Non-Recurring Costs

Other Non-Recurring Costs	
Shipping & Handling (From Day1 to Cloud Hosting provider only)	Rate
FedEx Ground	Standard Rates apply
FedEx Priority	Standard Rates apply
FedEx Standard Overnight	Standard Rates apply
FedEx Priority Overnight	Standard Rates apply

### 1.17 Cost Schedule Assumptions

1. Day1 has provided a 2% discount on AWS products and services outlined in the Cost Schedule.
2. All products and services associated with this agreement are considered tax exempt.
3. "Dedicated Fixed Price" resources are based upon pricing of assets that must reside in the GovCloud Region of AWS. Other Regions are available at request, although prices are subject to change.
4. Services and service options may not be available in all regions. Detailed information on available AWS services by region is available at
5. <http://aws.amazon.com/about-aws/globalinfrastructure/regional-product-services/>.
6. Other AWS products are available; prices will be provided at request and can be negotiated at the Engagement Addendum Level.
7. AWS Marketplace Products and Solutions are available at request.

## 2.0 Appendix A – Sample Infor SaaS Agreement

---

### SUBSCRIPTION LICENSE AND SERVICES AGREEMENT

AGREEMENT NUMBER:

**THIS SUBSCRIPTION LICENSE AND SERVICES AGREEMENT** (the “Agreement”) is between \_\_\_\_\_ (“Vendor”) and \_\_\_\_\_ (“End User”) as of the Effective Date. The parties agree as follows:

#### 1. Definitions.

(a) “**Affiliate**” means any entity, directly or indirectly, controlling, controlled by, or under common control with, Vendor.

(b) “**Authorized Users**” means: (i) Licensee’s employees; and (ii) contractors authorized by Licensee to access the Subscription Software who, prior to obtaining access to the Subscription Software, have executed a non-disclosure agreement that protects Vendor’s Confidential Information to the same extent as this Agreement, in each case registered in the database with a unique UserID and a unique password.

(c) “**Confidential Information**” means non-public information that is identified as or would be reasonably understood to be confidential and/or proprietary. Confidential Information of Vendor includes, without limitation, the Documentation and the Subscription Software, including any software code and all algorithms, methods, techniques, and processes revealed or utilized therein. Confidential Information of Licensee includes Licensee Data. Confidential Information does not include information that: (i) is or becomes known to the public without fault or breach of the Recipient; (ii) the Discloser regularly discloses to third parties without restriction on disclosure; (iii) the Recipient obtains from a third party without restriction on disclosure and without breach of a non-disclosure obligation known to Recipient; or (iv) is independently developed by the Recipient without use of Confidential Information.

(d) “**Discloser**” means the party providing Confidential Information to the Recipient.

(e) “**Documentation**” means the then-current Vendor-provided documentation relating to the features, functions, and use of the Subscription Software.

(f) “**Documented Defect**” means a material deviation between the then-current, general release version of the Subscription Software and its Documentation.

(g) “**Effective Date**” means the date identified on the signature page of this Agreement as the Effective Date.

(h) “**Initial Subscription Term**” means the initial subscription period set forth on the applicable Order Form.

(i) “**Intellectual Property Rights**” means any and all rights in patents, copyrights, trademarks and service marks.

(j) “**Licensee Data**” means information provided, entered or uploaded for use by or with the Subscription Software by the Licensee or its Authorized Users.

(k) “**License Restriction**” means any limitation on the use of the Subscription Software identified in an Order Form (e.g., number of Authorized Users, locations, connections).

(l) “**Order Form**” means each order form between the parties incorporating the terms of this Agreement which shall contain, without limitation, a list of the Subscription Software and associated quantity and License Restriction, a description of the Subscription Services, Subscription Fees, and payment terms.

(m) “**Personal Information**” means information provided to Vendor by or at the direction of Licensee, or to which access was provided to Vendor in the course of Vendor’s performance under this Agreement that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, financial account numbers, credit report information, biometric or health data, answers to security questions and other personal identifiers). Personal Information shall include any non-public personal information regarding any individual that is



subject to applicable national, state, regional, and/or local laws and regulations governing the privacy, security, confidentiality and protection of non-public personal information.

- (n) "**Recipient**" means the party receiving Confidential Information of the Discloser.
- (o) "**Renewal Term**" means any renewal or extension of Licensee's license to use the Subscription Software following the expiration of the Initial Subscription Term.
- (p) "**Residual Knowledge**" shall mean ideas, concepts, know-how or techniques related to the Discloser's technology and Confidential Information that are retained in the unaided memories of the Recipient who had rightful access to Confidential Information.
- (q) "**Service Level Description**" means the Service Level Description document applicable to the Subscription Services and attached as an exhibit to an Order Form.
- (r) "**Subscription Fees**" means the fees for the Subscription Services set forth on the applicable Order Form.
- (s) "**Subscription Services**" means the Subscription Software-related application hosting services and Support (as defined in Section 3(b)) that Vendor provides Licensee under this Agreement. At its sole discretion, Vendor may subcontract to a Third Party Licensor the obligation to provide the Subscription Services to Licensee; provided however, that Vendor will remain fully responsible for the provision of such Subscription Services in accordance with this Agreement.
- (t) "**Subscription Software**" means collectively or individually the computer software programs identified in the applicable Order Form for which Vendor is providing the Subscription Services.
- (u) "**Subscription Term**" means the Initial Subscription Term or any Renewal Term, as applicable.
- (v) "**Third Party Licensor**" means a third party whose software products ("**Third Party Products**") have been made available to Vendor for distribution and licensing under the terms of its agreement with such Third Party Licensor (a "**Third Party Agreement**"). Licensee acknowledges and agrees that any such Third Party Licensor is a third party beneficiary to this Agreement with respect to enforcing Licensee's obligations related to the Subscription Software and Subscription Services
- (w) "**Updates**" means generally available updates, enhancements or modifications to the then-current, general release version of the Subscription Software that are not separately priced or licensed as new products.
- (x) "**UserID**" means a unique user identification credential used in combination with a unique password to access the Subscription Services.

**2. License.** Subject to the terms and conditions of this Agreement and the applicable Order Form, Vendor hereby grants to Licensee a non-exclusive, non-transferable, limited license (without the right to sublease or sublicense) to access and use the Subscription Software and the Subscription Services, during the Subscription Term, in an operating environment hosted by Vendor, for Licensee's own internal use. Any rights not expressly granted in this Agreement are expressly reserved.

(a) **Documentation.** Licensee may make a reasonable number of copies of the Documentation for the Subscription Software for its internal use in accordance with the terms of this Agreement.

(b) **License Restriction.** Licensee's use of the Subscription Software and Subscription Services is subject to any License Restriction specified in the applicable Order Form.

(c) **Additional Restrictions on Use of the Subscription Software and Subscription Services.** In no event shall Licensee access the Subscription Software on any environment outside the hosted environment selected by Vendor as part of the Subscription Services. In no event shall Licensee or its Authorized Users possess or control the Subscription Software or any related software code. Licensee is prohibited from causing or permitting the reverse engineering, disassembly or de-compilation of the Subscription Software. Except as expressly provided by this Agreement, Licensee is prohibited from using the Subscription Software to provide service bureau services to third parties. Licensee will not allow the Subscription Software to be used by, or disclose all or any part of the Subscription Software to, any person except Authorized Users. Licensee acknowledges and agrees that U.S. export control laws and other applicable export and import laws govern its use of the Subscription Software and Licensee will neither export or re-export, directly or

indirectly, the Subscription Software, nor any direct product thereof in violation of such laws, or use the Subscription Software for any purpose prohibited by such laws.

(d) Intellectual Property Rights Notices. Licensee is prohibited from removing or altering any of the Intellectual Property Rights notice(s) embedded in the Subscription Software or that Vendor otherwise provides with the Subscription Services. Licensee must reproduce the unaltered Intellectual Property Rights notice(s) in any full or partial copies that Licensee makes of the Documentation.

(e) Ownership. Use of the Subscription Software and Subscription Services does not grant any ownership rights in or to the Subscription Software, the Subscription Services, or the Documentation. Licensee Data shall be the sole property of Licensee; however, Infor may aggregate anonymous statistical data regarding use and functioning of its system by its various licensees, and all such data (none of which shall be considered Licensee Data), will be the sole property of Infor.

### **3. Subscription Services.**

(a) Hosted Environment. Vendor will provide the application hosting environment, including the hardware, equipment, and systems software configuration on which Vendor supports use of the Subscription Software and Subscription Services, on servers located at a facility selected by Vendor.

(b) Support. Vendor shall (a) provide Licensee with access (via the internet, telephone or other means established by Vendor) to Vendor's support helpline, (b) install, when and if generally available, Updates; and (c) use reasonable efforts to correct or circumvent any material deviation between the then-current, general release version of the Subscription Software and its Documentation (the foregoing referred to collectively as "Support"). Support is included in the Subscription Fee.

(c) User Accounts. Licensee is responsible for maintaining its own Authorized User UserIDs and passwords which can be managed through the Subscription Software interface. Licensee is responsible for maintaining the confidentiality of Licensee's UserIDs and passwords and shall cause its Authorized Users to maintain the confidentiality of their UserIDs and Passwords. Licensee is responsible for all uses of and activities undertaken with UserIDs registered on Licensee's account. Licensee agrees to immediately notify Vendor of any unauthorized use of Licensee's UserIDs of which Licensee becomes aware.

(d) Connectivity. Vendor will be responsible for maintaining connectivity from its network to the Internet which is capable of servicing the relevant Internet traffic to and from the hosted environment. Licensee is responsible for providing connectivity to the Internet for itself and its Authorized Users. Licensee shall also be responsible for ensuring that latency and available bandwidth from the user's desktop to Vendor's hosted routers is adequate to meet Licensee's desired level of performance. If Licensee requires a VPN or private network connection to the Subscription Services, Licensee is responsible for all costs associated with any specialized network connectivity required by Licensee.

(e) Restrictions. Vendor shall have no obligation to correct a problem caused by Licensee's negligence, Licensee's equipment malfunction or other causes beyond the control of Vendor.

### **4. Payment and Taxes.**

(a) Payment. Licensee shall pay Vendor the Subscription Fees set forth on the Order Form. Subscription Fees are payable in advance and Vendor will invoice Licensee for Subscription Fees prior to the commencement of the portion of the Subscription Term to which such fees apply. After the Initial Subscription Term, the Subscription Fees shall be subject to annual adjustment. Except as otherwise set forth in this Agreement, Subscription Fees are non-refundable. Licensee will pay each Vendor invoice in accordance with the payment terms set forth on the Order Form. Late payments are subject to a late charge equal to the lesser of: (i) one and one-half percent (1½%) per month; and (ii) the highest rate permitted by applicable law. Notwithstanding anything to the contrary in this Agreement, Vendor reserves the right to suspend access to the Subscription Services in the event of any past due Subscription Fees.

(b) Taxes. Licensee is responsible for paying all taxes relating to this Agreement (except for taxes based on Vendor's net income or capital stock). Applicable tax amounts (if any) are not included in the Subscription Fees set forth on any Order Form. Vendor will invoice Licensee for applicable tax amounts and such invoices are payable in accordance with Section 4(a) and the Order Form.

### **5. Limited Warranties, Disclaimer of Warranties, and Remedies.**

(a) Right to Grant License. Vendor warrants that it has obtained rights in the Subscription Software sufficient to grant the licenses granted to Licensee under this Agreement. Licensee's exclusive remedy, and Vendor's exclusive obligation, for a breach of this warranty is set forth in Section 7 (Indemnity).

(b) Limited Subscription Software Warranty by Vendor and Remedy For Breach. Vendor warrants that the Subscription Software licensed to Licensee will operate without a Documented Defect for a period of ninety (90) days from the applicable Subscription Service Ready Date defined in the applicable Order Form. Vendor's sole obligation with respect to a breach of the foregoing warranty shall be to repair or replace the Subscription Software giving rise to the breach of warranty. If Vendor is unable to repair or replace such Subscription Software within a reasonable period of time, then, subject to the limitations set forth in Section 14 of this Agreement, Licensee may pursue its remedies at law to recover direct damages resulting from the breach of this warranty. The remedies in this Section 5(b) are exclusive and in lieu of all other remedies, and represent Vendor's sole obligations, for a breach of the foregoing warranty. Licensee must provide notice to Vendor of any warranty claim within the warranty period. For clarity, Licensee's entitlement to Support (as defined in Section 3(b)) in connection with any Documented Defect shall continue throughout the Subscription Term.

(c) Malicious Code. Vendor represents that it has used commercially reasonable best efforts utilizing generally accepted industry tools and practices to provide Subscription Software that does not contain any "time bombs," "worms," "viruses," "Trojan horses," "protect codes," "data destruct keys," or other programming devices that are intended to access, modify, delete, damage, deactivate or disable the Subscription Services ("Malicious Code"). As Licensee's sole remedy for breach of this representation, Vendor shall take action immediately to investigate, identify and remove such Malicious Code from the Subscription Software.

(d) Limited Services Warranty and Remedy For Breach. Vendor warrants to Licensee that, Vendor will render the Subscription Services with commercially reasonable care and skill. Vendor further warrants that the hosted environment will be available at all times throughout the Subscription Term, subject to the exceptions and allowances described in the Availability section of the applicable Service Level Description. The level of unavailability shall not exceed one half of one percent (0.5%) per month, excluding Scheduled Maintenance as described in the applicable Service Level Description (the "Down Time Warranty"). In the event of a breach of the foregoing warranty Vendor shall apply service level credits based on the actual availability measure for the applicable period as follows:

<u>Availability</u>	<u>Service Level Credit</u>
99.500% or greater	No Service Level Credit
99.499% - 99.000%	5% of the monthly prorated subscription fee
98.999% - 98.500%	15% of the monthly prorated subscription fee
98.499% - 95.000%	25% of the monthly prorated subscription fee
Below 95.000%	35% of the monthly prorated subscription fee

Service level credits for Subscription Fees paid on an annual or quarterly basis shall be based on a monthly equivalent fee. For example, a 5% service level credit on an annual subscription fee shall be 5% of 1/12 of the annual fee. Service level credits shall be applied to Licensee's next invoice or, if Licensee has paid the final invoice under this Agreement, service level credits shall be paid to Licensee within thirty (30) calendar days following the determination that the credit is due. The service level credit is the exclusive remedy and is in lieu of all other remedies for breach of the Down Time Warranty.

(e) Disclaimer of Warranties. The limited warranties in this Section 5 are made to Licensee exclusively and are in lieu of all other warranties. **VENDOR AND ITS THIRD PARTY LICENSORS MAKE NO OTHER WARRANTIES WHATSOEVER, EXPRESS OR IMPLIED, WITH REGARD TO THE SUBSCRIPTION SOFTWARE AND SUBSCRIPTION SERVICES PROVIDED UNDER THIS AGREEMENT AND/OR ANY ORDER FORM, IN WHOLE OR**

**IN PART. VENDOR AND ITS THIRD PARTY LICENSORS EXPLICITLY DISCLAIM ALL WARRANTIES OF MERCHANTABILITY AND OF FITNESS FOR A PARTICULAR PURPOSE. VENDOR AND ITS THIRD PARTY LICENSORS EXPRESSLY DO NOT WARRANT THAT THE SUBSCRIPTION SOFTWARE OR SUBSCRIPTION SERVICES, IN WHOLE OR IN PART, WILL BE ERROR FREE, OPERATE WITHOUT INTERRUPTION OR MEET LICENSEE'S REQUIREMENTS.**

(f) Abrogation of Limited Warranty. Vendor will have no obligation under this Section 5 to the extent that any alleged breach of warranty is caused by any modification of the Subscription Software not performed by or on behalf of Vendor. To the extent that an alleged breach of warranty concerns a Third Party Product that is subject to a more limited warranty under a Third Party Agreement than specified in Section 5 above, Vendor's obligations hereunder will be further limited accordingly.

(g) **FAILURE OF ESSENTIAL PURPOSE. THE PARTIES HAVE AGREED THAT THE LIMITATIONS SPECIFIED IN SECTIONS 5 AND 14 WILL SURVIVE AND APPLY EVEN IF ANY REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE, AND REGARDLESS OF WHETHER LICENSEE HAS ACCEPTED ANY SUBSCRIPTION SOFTWARE OR SUBSCRIPTION SERVICE UNDER THIS AGREEMENT.**

(h) **HIGH RISK ACTIVITIES. THE SUBSCRIPTION SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE AS ON-LINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR AIRCRAFT COMMUNICATION SYSTEMS, MASS TRANSIT, AIR TRAFFIC CONTROL, DIRECT LIFE SUPPORT MACHINES, OR WEAPONS SYSTEMS, IN WHICH THE FAILURE OF THE SUBSCRIPTION SOFTWARE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). ACCORDINGLY, VENDOR AND ITS THIRD PARTY LICENSORS DISCLAIM ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES. LICENSEE AGREES THAT VENDOR AND ITS THIRD PARTY LICENSORS SHALL NOT BE LIABLE FOR ANY CLAIMS OR DAMAGES ARISING FROM OR RELATED TO THE USE OF THE SUBSCRIPTION SOFTWARE IN SUCH APPLICATIONS.**

## **6. Confidential Information.**

(a) Confidentiality. The Confidential Information disclosed under this Agreement may be used, disclosed or reproduced only to the extent necessary to further and fulfill the purposes of this Agreement. Except as otherwise permitted under this Agreement, the Recipient will not knowingly disclose to any third party, or make any use of the Discloser's Confidential Information. The Recipient will use at least the same standard of care to maintain the confidentiality of the Discloser's Confidential Information that it uses to maintain the confidentiality of its own Confidential Information, but in no event less than reasonable care. The non-disclosure and non-use obligations of this Agreement will remain in full force with respect to each item of Confidential Information for a period of ten (10) years after Recipient's receipt of that item; provided, however, that Licensee's obligations to maintain the Subscription Software and Documentation as confidential will survive in perpetuity. Each of Licensee and Vendor shall be responsible for the breach of the confidentiality terms contained in this Section 6 by any of its directors, officers, employees, Authorized Users, agents, accountants and advisors. Notwithstanding the foregoing, this Section is not intended to prevent (a) a Recipient from using Residual Knowledge, subject to any Intellectual Property Rights of the Discloser, or (b) Vendor or its Third Party Licensor's from using aggregated data regarding the use of the Subscription Services to provide reports or analytics to Licensee or to improve the performance of Vendor's or such Third Party Licensor's products, provided such data does not contain any Personal Information regarding Licensee, its employees, customers or Authorized Users. If the Recipient should receive any legal request or process in any form seeking disclosure of Discloser's Confidential Information, or if the Recipient should be advised by counsel of any obligation to disclose such Confidential Information, the Recipient shall (if allowed by law) provide the Discloser with prompt notice of such request or advice so that the Discloser may seek a protective order or pursue other appropriate assurance of the confidential treatment of the Confidential Information. Regardless of whether or not a protective order or other assurance is obtained, the Recipient shall furnish only that portion of the Discloser's Confidential Information which is legally required to be furnished and to use reasonable efforts to assure that the information is maintained in confidence by the party to whom it is furnished.

(b) Security Policies and Safeguards. Vendor shall establish and maintain administrative, technical, and physical safeguards designed to protect against the destruction, loss, unauthorized access or alteration of Licensee Data and Personal Information in the possession or under the control of Vendor or to which Vendor has access, which are: (i) no less rigorous than those maintained by Vendor for its own information of a similar nature; (ii) no less rigorous than generally accepted industry standards; and (iii) required by applicable laws. The security procedures and safeguards implemented and maintained by Vendor pursuant to this Section 6(b) shall include, without limitation:

- (i) User identification and access controls designed to limit access to Licensee's Data to authorized users;

- (ii) the use of appropriate procedures and technical controls regulating data entering Vendor's network from any external source;
- (iii) the use of encryption techniques when Licensee's Data is transmitted or transferred into or out of the hosted environment;
- (iv) physical security measures, including without limitation securing Licensee's Data within a secure facility where only authorized personnel and agents will have physical access to Licensee Data;
- (v) operational measures, including without limitation IT Service Management (ITSM) processes designed to ensure the correct and secure operations of information processing activities;
- (v) periodic employee training regarding the security programs referenced in this Section; and
- (vi) periodic testing of the systems and procedures outlined in this Section.

(c) **Review of Controls.** Once in each 12 month period during the Subscription Term, Vendor shall, at its cost and expense, engage a duly qualified independent auditor to conduct a review of the design and operating effectiveness of Vendor's defined control objectives and control activities in connection with the Subscription Services. Vendor shall cause such auditor to prepare a report in accordance with the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 16 (SSAE 16) or an equivalent standard, which may include ISAE 3402 (the "Audit Report"). Licensee shall have the right to request and receive a copy of the Audit Report and Licensee may share a copy of such Audit Report with its auditors and regulators, provided that, such Audit Report shall be Vendor's Confidential Information (as defined in this Agreement).

(d) Security Incident Response. In the event that Vendor becomes aware that the security of any Licensee Data or Personal Information has been compromised, or that such Licensee Data or Personal Information has been or is reasonably expected to be subject to a use or disclosure not authorized by this Agreement (an "Information Security Incident"), Vendor shall: (i) promptly (and in any event within 24 hours of becoming aware of such Information Security Incident), notify Licensee, in writing, of the occurrence of such Information Security Incident; (ii) investigate such Information Security Incident and conduct a reasonable analysis of the cause(s) of such Information Security Incident; (iii) provide periodic updates of any ongoing investigation to Licensee; (iv) develop and implement an appropriate plan to remediate the cause of such Information Security Incident to the extent such cause is within Vendor's control; and (v) cooperate with Licensee's reasonable investigation or Licensee's efforts to comply with any notification or other regulatory requirements applicable to such Information Security Incident.

**7. Indemnity by Vendor.** Vendor will defend, indemnify and hold Licensee harmless from and against any loss, cost and expense to the extent arising from a third party claim against Licensee that the Subscription Software infringes any Intellectual Property Rights of others. Vendor's obligations under this indemnification are expressly conditioned on the following: (i) Licensee must promptly notify Vendor of any such claim; (ii) Licensee must, in writing, grant Vendor sole control of the defense of any such claim and of all negotiations for its settlement or compromise so long as such settlement or compromise does not result in payment of money by Licensee or an admission of guilt by Licensee (if Licensee chooses to represent its own interests in any such action, Licensee may do so at its own expense, but such representation must not prejudice Vendor's right to control the defense of the claim and negotiate its settlement or compromise); (iii) Licensee must reasonably cooperate with Vendor to facilitate the settlement or defense of the claim. Vendor will not have any liability hereunder to the extent the claim arises from (a) any modification of the Subscription Software by, on behalf of, or at the request of Licensee; or (b) the use or combination of the Subscription Software with any computer, computer platform, operating system and/or data base management system other than provided by Vendor. If any Subscription Software is, or in Vendor's opinion is likely to become, the subject of an Intellectual Property Rights infringement claim, then Vendor, at its sole option and expense, will either: (A) obtain for Licensee the right to continue using the Subscription Software under the terms of this Agreement; (B) replace the Subscription Software with products that are substantially equivalent in function, or modify the Subscription Software so that it becomes non-infringing and substantially equivalent in function; or (C) refund to Licensee the un-used portion of the Subscription Services fee, if any, paid to Vendor for the Subscription Software giving rise to the infringement claim, and discontinue Licensee's use of such Subscription Software. **THE FOREGOING SETS FORTH VENDOR'S AND ITS THIRD PARTY LICENSORS' EXCLUSIVE OBLIGATION AND LIABILITY WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.**

## **8. Term and Termination.**

(a) **Term.** With respect to the Subscription Software, the Initial Subscription Term shall be as set forth on the applicable Order Form. After the Initial Subscription Term, the Subscription Term shall automatically renew for successive one-year Renewal Terms, unless either party provides written notice of non-renewal to the other party at least ninety (90) days prior to expiration of the Initial Subscription Term or then current Renewal Term, as the case may be. Except as set forth in Section 8(b), the Subscription Term cannot be terminated prior to its expiration date.

(b) **Right of Termination.** If either party breaches any material obligation in this Agreement or an Order Form (including, without limitation, any obligation to pay Subscription Fees), and fails to remedy such breach (if such breach can be remedied) within thirty (30) days of receipt of written notice of such breach, the other party may terminate this Agreement (including all Order Forms hereunder). Notwithstanding the foregoing, to the extent such material breach cannot be remedied through efforts of the breaching party, the other party has the right to terminate this Agreement (including all Order Forms hereunder) on less than thirty days' written notice.

(c) **Effect of Termination.** Upon termination of this Agreement by either party, Licensee's license to access and use the Subscription Software and Subscription Services shall immediately terminate as of the effective date of such termination. Termination of this Agreement will not release either party from making payments which may be owing to the other party under the terms of this Agreement through the effective date of such termination. Termination of this Agreement will be without prejudice to the terminating party's other rights and remedies pursuant to this Agreement, unless otherwise expressly stated herein.

(d) **Return of Licensee Data.** Upon termination or expiration of this Agreement, Vendor shall promptly make all Licensee Data available to Licensee as a native database export provided through Vendor's FTP server. In the event that Licensee requires the return of Licensee Data in an alternate format or requires any other termination assistance services, Vendor and Licensee shall mutually agree upon the scope of such termination assistance services and the fees and expenses payable for such termination assistance services.

(e) **Survival of Obligations.** All obligations relating to non-use and non-disclosure of Confidential Information, limitation of liability, and such other terms which by their nature survive termination, will survive termination or expiration of this Agreement.

**9. Notices.** All notices and other communications required or permitted under this Agreement must be in writing and will be deemed given when: delivered personally; sent by registered or certified mail, return receipt requested; transmitted by facsimile confirmed by first class mail; or sent by overnight courier. Notices must be sent to a party at its address shown on the signature page of this Agreement, or to such other place as the party may subsequently designate for its receipt of notices in accordance with this Section. Licensee must promptly send copies of any notice of material breach and/or termination of the Agreement to Vendor, Attention: \_\_\_\_\_, or to such other place as Vendor may subsequently designate for its receipt of notices.

**10. Force Majeure.** Except with respect to the payment of fees hereunder, neither party will be liable to the other for any failure or delay in performance under this Agreement due to circumstances beyond its reasonable control, including, without limitation, Acts of God, war, terrorist acts, accident, labor disruption, acts, omissions and defaults of third parties and official, governmental and judicial action not the fault of the party failing or delaying in performance, or the threat of any of the foregoing.

**11. Assignment.** Licensee may not assign or transfer any of its rights or obligations under this Agreement without the prior written consent of Vendor, whether by operation of law or otherwise, including in connection with a change in control, merger, acquisition, consolidation, asset sale or other reorganization, and any attempt at such assignment or transfer will be void.

**12. No Waiver.** A party's failure to enforce its rights with respect to any single or continuing breach of this Agreement will not act as a waiver of the right of that party to later enforce any such rights or to enforce any other or any subsequent breach.

**13. Choice of Law; Severability.** This Agreement shall be governed by and interpreted in accordance with the laws of the State of New York, without application of any conflict of laws provisions thereof, and all claims relating to or arising out of this Agreement, or the breach thereof, whether sounding in contract, tort or otherwise, shall likewise be governed by the laws of the State of New York, without application of any conflict of laws provisions thereof. This Agreement is originally written in the English language and the English language version shall control over any translations. If any provision of this Agreement is illegal or unenforceable, it will be deemed stricken from the Agreement and the remaining provisions of the Agreement will remain in full force and effect. The United Nations Convention on the International Sale of Goods (CISG) shall not apply to the interpretation or enforcement of this Agreement.

#### **14. LIMITATIONS OF LIABILITY.**

**(a) LIMITED LIABILITY OF VENDOR. EXCEPT WITH RESPECT TO INTELLECTUAL PROPERTY INDEMNIFICATION OBLIGATIONS UNDER SECTION 7, THE TOTAL LIABILITY OF VENDOR, ITS AFFILIATES AND THIRD PARTY LICENSORS IN CONNECTION WITH OR RELATED TO THE SUBSCRIPTION SOFTWARE, THE SUBSCRIPTION SERVICES, OR ANY OTHER MATTER RELATING TO THIS AGREEMENT (WHATEVER THE**

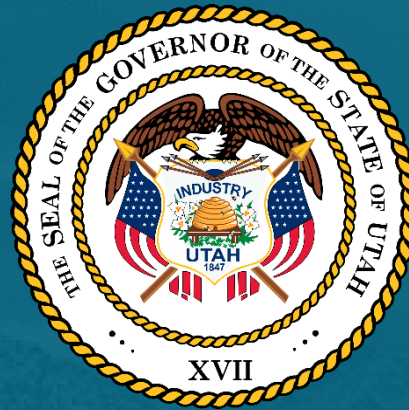
**BASIS FOR THE CAUSE OF ACTION) WILL NOT EXCEED THE SUBSCRIPTION FEES PAID OR PAYABLE TO VENDOR HEREUNDER FOR THE TWELVE-MONTH PERIOD IN WHICH SUCH LIABILITY FIRST AROSE.**

**(b) EXCLUSION OF DAMAGES. IN NO EVENT WILL VENDOR, ITS AFFILIATES OR THIRD PARTY LICENSORS BE LIABLE FOR ANY SPECIAL, PUNITIVE, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, AND REGARDLESS OF WHETHER VENDOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE.**

**15. Audit Rights.** Vendor (including any third party auditor retained by Vendor) may audit the records and systems of Licensee to ensure compliance with the terms of this Agreement and each applicable Order Form. Vendor will notify Licensee in writing at least ten (10) business days prior to any such audit. Any such audit will be conducted during regular business hours and will not interfere unreasonably with Licensee's business activities. Vendor may audit Licensee no more than once in any twelve (12) month period. If an audit reveals that Licensee is using the Subscription Software or Subscription Services beyond the scope of the license granted herein (for example, in excess of the License Restriction), then, in addition to any other remedies available to Vendor, Licensee will promptly pay Vendor the underpaid Subscription Fees associated therewith based on Vendor's then-current list rates, as well as any applicable late charges.

**16. Compliance with Laws.** Licensee will comply with all laws, rules and regulations applicable to the use of the Subscription Software and the Subscription Services including, without limitation, by not submitting any Licensee Data that is illegal, defamatory, or that infringes any third party proprietary rights.

**17. Entire Agreement.** This Agreement contains the entire understanding of the parties with respect to its subject matter, and supersedes and extinguishes all prior oral and written communications between the parties about its subject matter. Any purchase order or similar document, which may be issued by Licensee in connection with this Agreement, does not modify, supplement or add terms to this Agreement. No modification of this Agreement will be effective unless it is in writing, is signed by each party, and expressly provides that it amends this Agreement. This Agreement and any signed agreement or instrument entered into in connection herewith or contemplated hereby, and any amendments hereto or thereto, to the extent signed and delivered by means of digital imaging, electronic mail or a facsimile machine, shall be treated in all manner and respects as an original agreement or instrument and shall be considered to have the same binding legal effect as if it were the original signed version thereof delivered in person. This Agreement and all Order Forms may be signed in counterparts.



State of Utah Division of Purchasing

**NASPO VALUEPOINT MASTER AGREEMENT  
FOR CLOUD SOLUTION**

CH16012

**TECHNICAL RESPONSE**





# Contents

1.0	Technical Response [RFP Section 8]	5
1.1	(M)(E) Technical Requirements [RFP 8.1]	5
1.1.1	Cloud Service Model(s) and Deployment Model(s) [RFP 8.1.1]	5
1.1.2	NIST Characteristics [RFP 8.1.2]	8
1.1.3	Subcategory(ies) [RFP 8.1.3]	15
1.1.4	Compliance with Attachments C & D [RFP 8.1.4]	16
1.1.5	Adherence to Services, Definitions and Deployment Models in Attachment D [RFP 8.1.5]	17
1.2	(E) Subcontractors [RFP 8.2]	17
1.2.1	Direct Delivery or Subcontractors [RFP 8.2.1]	17
1.2.2	Subcontractor Usage [RFP 8.2.2]	19
1.2.3	Subcontractor Qualifications [RFP 8.2.3]	19
1.3	(E) Working with Purchasing Entities [RFP 8.3]	20
1.3.1	Working with Purchasing Entities through Data Breaches [RFP 8.3.1]	20
1.3.2	Adware, Software or Marketing [RFP 8.3.2]	23
1.3.3	Test/Staging Environment [RFP 8.3.3]	23
1.3.4	Accessibility [RFP 8.3.4]	23
1.3.5	Web Browsers [RFP 8.3.5]	24
1.3.6	Meeting Purchasing Entities [RFP 8.3.6]	25
1.3.7	Project Schedule Plans [RFP 8.3.7]	25
1.4	(E) Customer Service [RFP 8.4]	27
1.4.1	Customer Service [RFP 8.4.1]	29
1.4.2	Customer Service Requirements [RFP 8.4.2]	35
1.5	(E) Security of Information [RFP 8.5]	39
1.5.1	Data Protection [RFP 8.5.1]	39
1.5.2	Comply with Applicable Laws [RFP 8.5.2]	41
1.5.3	Accessing Purchasing Entity's user accounts or data [RFP 8.5.3]	42
1.6	(E) Privacy and Security [RFP 8.6]	42
1.6.1	Commitment to Industry Standards [RFP 8.6.1]	42
1.6.2	Organization Security Certifications [RFP 8.6.2]	42

1.6.3	Security Practices [RFP 8.6.3].....	43
1.6.4	Data Confidentiality Standards [RFP 8.6.4].....	45
1.6.5	Third-Party attestations, Reports, Security Credentials, and Certifications [RFP 8.6.5] .....	46
1.6.6	Logging Process [RFP 8.6.6] .....	46
1.6.7	Visibility Restriction [RFP 8.6.7] .....	47
1.6.8	Security Incident Notification Process [RFP 8.6.8].....	47
1.6.9	Security Controls [RFP 8.6.9] .....	48
1.6.10	Security Technical Reference Architecture [RFP 8.6.10] .....	48
1.6.11	Security Procedures [RFP 8.6.11] .....	49
1.6.12	Security Measures and Standards [RFP 8.6.12].....	49
1.6.13	Notification Policies and Procedures [RFP 8.6.13] .....	50
1.7	(E) Migration and Redeployment Plan [RFP 8.7].....	50
1.7.1	End of Life Activities [RFP 8.7.1] .....	50
1.7.2	Return of Data [RFP 8.7.2] .....	51
1.8	(E) Service or Data Recovery [RFP 8.8].....	51
1.8.1	Situational Response [RFP 8.8.1] .....	51
1.8.2	Backup and Restore Methodology [RFP 8.8.2] .....	52
1.9	(E) Data Protection [RFP 8.9].....	54
1.9.1	Encryption Technologies [RFP 8.9.1] .....	54
1.9.2	Business Associate Agreement [RFP 8.9.2] .....	55
1.9.3	Data use in alignment with Master Agreement [RFP 8.9.3] .....	55
1.10	(E) Service Level Agreements [RFP 8.10].....	55
1.10.1	Negotiable SLA [RFP 8.10.1] .....	55
1.10.2	Sample SLA [RFP 8.10.2] .....	56
1.11	(E) Data Disposal [RFP 8.11].....	56
1.12	(E) Performance Measures and Reporting [RFP 8.12].....	57
1.12.1	Guarantee Reliability [RFP 8.12.1].....	57
1.12.2	Standard Uptime [RFP 8.12.2].....	57
1.12.3	Support Process [RFP 8.12.3] .....	58
1.12.4	Consequences for Not Meeting SLA Standard for Response Time and Incident Fix Time [RFP 8.12.4]	62
1.12.5	Planned Downtime [RFP 8.12.5].....	62
1.12.6	Consequences for Not Meeting SLA Standard for Disaster Recovery [RFP 8.12.6] .....	64

1.12.7	Sample Performance Reports [RFP 8.12.7] .....	65
1.12.8	Report Printing [RFP 8.12.8] .....	67
1.12.9	On-Demand Deployment [RFP 8.12.9] .....	67
1.12.10	Scale-up and Scale-Down [RFP 8.12.10] .....	67
1.13	(E) Cloud Security Alliance Questionnaires [RFP 8.13] .....	68
1.14	(E) Service Provisioning [RFP 8.14] .....	68
1.14.1	Emergency/Rush Service Implementation [RFP 8.14.1] .....	69
1.14.2	Lead-Time for Provisioning [RFP 8.14.2] .....	69
1.15	(E) Back Up and Disaster Plan [RFP 8.15] .....	70
1.15.1	Methodologies for Backup and Restore Services [RFP 8.15.1] .....	70
1.15.2	Inherent Disaster Recovery Risks [RFP 8.15.2] .....	70
1.15.3	Multi Data Center Infrastructure Support [RFP 8.15.3] .....	72
1.16	(E) Solution Administration [RFP 8.16] .....	73
1.16.1	Managing Identity and User Accounts [RFP 8.16.1] .....	73
1.16.2	Anti-Virus Protection [RFP 8.16.2] .....	74
1.16.3	Data Migration [RFP 8.16.3] .....	74
1.16.4	Administering the Solution [RFP 8.16.4] .....	74
1.16.5	Defined Administration Policies [RFP 8.16.5] .....	74
1.17	(E) Hosting and Provisioning [RFP 8.17] .....	75
1.17.1	Cloud hosting Provisioning Process [RFP 8.17.1] .....	75
1.17.2	Provided Tool Sets [RFP 8.17.2] .....	76
1.18	(E) Trial and Testing Periods (Pre- and Post-Purchase) [RFP 8.18] .....	78
1.18.1	Testing and Training Periods [RFP 8.18.1] .....	78
1.18.2	Test and POC environments [RFP 8.18.2] .....	78
1.18.3	Training and Support [RFP 8.18.3] .....	79
1.19	(E) Integration and Customization [RFP 8.19] .....	79
1.19.1	Service Integration [RFP 8.19.1] .....	79
1.19.2	Customize and Personalize Solutions [RFP 8.19.2] .....	82
1.20	(E) Marketing Plan [RFP 8.20] .....	83
1.21	(E) Related Value-Added Services to Cloud Solutions [RFP 8.21] .....	85
1.22	(E) Supporting Infrastructure [RFP 8.22] .....	92
1.22.1	Purchasing Entity Required Infrastructure [RFP 8.22.1] .....	92
1.22.2	Installation of new Infrastructure Responsibility Model [RFP 8.22.2] .....	93

1.23	(E) Alignment of Cloud Computing Reference Architecture [RFP 8.23] .....	94
2.0	Appendix A .....	95

## 1.0 Technical Response [RFP Section 8]

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

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

### 1.1 (M)(E) Technical Requirements [RFP 8.1]

#### 1.1.1 Cloud Service Model(s) and Deployment Model(s) [RFP 8.1.1]

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

As an Amazon Web Services, Inc. (AWS) Authorized reseller, Day1 provides NASPO with direct access to the expansive catalog of services and solutions provided by AWS, including the AWS Marketplace. AWS offers scalable, cost-efficient cloud services that NASPO can use to meet governance and security mandates, reduce costs, drive efficiencies, and accelerate innovation for its customers. Additionally, Day1 holds the necessary partnership levels with AWS to offer a full scope of cloud services and solutions beyond resale, which include *Channel Reseller Partner, Advanced Consulting Partner, Managed Service Partner, Direct Connect Partner, Marketplace Reseller, Marketplace Consulting Partner, Big Data Competency, and Authorized Government*

*Partner* as seen in Figure 1 below. The impact of these partnership levels with AWS can be found in the bullets and Figure 2 below as it allows our organization the ability to provide comprehensive end-to-end cloud based solutions through an operating model that allows Day1 to serve as a Value Added Reseller (VAR), Systems Integrator (SI), and a Managed Service Provider (MSP) for AWS. Our achievements with these partnership levels demonstrate our ability to provide NASPO with certified staff, organizational competencies, and exclusive experience as an AWS cloud service provider. Leveraging AWS, we can provide NASPO and NASPO purchasing entities with the ability to implement all types of cloud, whether its Private, Public, Hybrid and Community cloud.

Day1 offers an expansive array of IaaS, PaaS and SaaS services through AWS in Private, Public or Hybrid cloud environments. Today, under our existing contract we offer all service models in partnership with AWS core framework (compute, storage, and network). We then offer our clients the ability to layer in PaaS and SaaS based solutions from the AWS Lambda, code deploy, and Marketplace. We also provide PaaS based offerings such as Lambda, code deploy, EC2 Containers to name a few.

#### WSCA PRIME CONTRACT HOLDER

Day1 is one of only four prime contract holders for [WSCA's Public Cloud Hosting Services](#) vehicle. This enables state, local and education agencies to bypass cumbersome procurement processes and implement innovative, cloud-based solutions at a discounted rate.



Figure 1: Day1's AWS Partnership Achievements

Day1 has extensive experience customizing cloud architectures for state, local, federal governments and enterprises and will bring our experiences to bare as we guide NASPO and NASPO purchasing entities in developing custom cloud solutions based on the deployment model of each customer. The cloud deployment models are as described below:

1. **Public:** A public cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
2. **Community:** Community cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
3. **Hybrid:** Hybrid cloud infrastructure is a composition of two or more cloud models (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Additionally, hybrid solutions can may also integrate with on-premise solutions.
4. **Private:** The cloud infrastructure is operated solely for an organization. Data, information, and security for this cloud model is strictly controlled, processed, and stored in the private infrastructure.

For NASPO, the Day1 business model offers a simplified approach to cloud delivery from procurement, design, integration, and through operations and maintenance with the use of a highly accredited cloud service provider. Additionally, our business model provides NASPO with decreased administrative overhead and management by ensuring a single point of contact for all cloud services, increased accountability through a single vendor, and complete end-to-end cloud services.

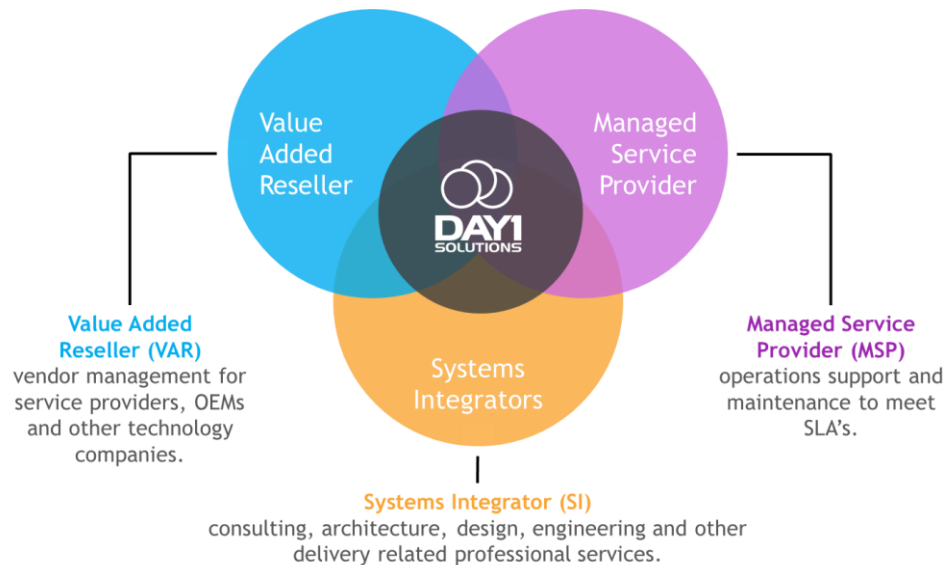


Figure 2: Day1's Business Model

- **Value Added Reseller (VAR):** As a Channel Reseller Partner, Day1 Solutions can provide NASPO direct access to the expansive catalog of services within AWS. Additionally, our extensive experience and partner level as a reseller provides NASPO with an organization adept to the complexities of vendor management with AWS.
- **Systems Integrator (SI):** Our competencies as an Advanced Consulting Partner ensure that Day1 can provide NASPO with a high-level of consulting, architecture, design, engineering and other delivery related professional services. Day1 has an abundance of AWS certified staff who continue to investigate new cloud offerings and pursue new solutions for IT efforts. Our continuous evolution of cloud services will allow NASPO to quickly innovate to new cutting edge IT solutions.
- **Managed Service Provider (MSP):** Our designation as an AWS Managed Service Provider provides NASPO with a great level of assurance that Day1 Solutions is appropriately equipped to manage all solutions developed within AWS. Our MSP practice ensures that the complexities of managing a cloud infrastructure are removed from NASPO as our teams will monitor operational support and maintenance to meet Service Level Agreements (SLA's).

As a revolutionary services company representing a new breed of CSP's, Day1 was created with the intent and goal of becoming a one-stop shop for customers to procure, design, implement, and maintain existing IT workloads in the AWS cloud. Day1 was founded by Mr. Luis Benavides who served as an executive for AWS and promoted this business model across all parts of the organization before eventually creating his own company. His focus was to develop the necessary partnership levels within AWS to guarantee a full scope of service delivery. Figure 3 below outlines our business lines, services and product offerings:

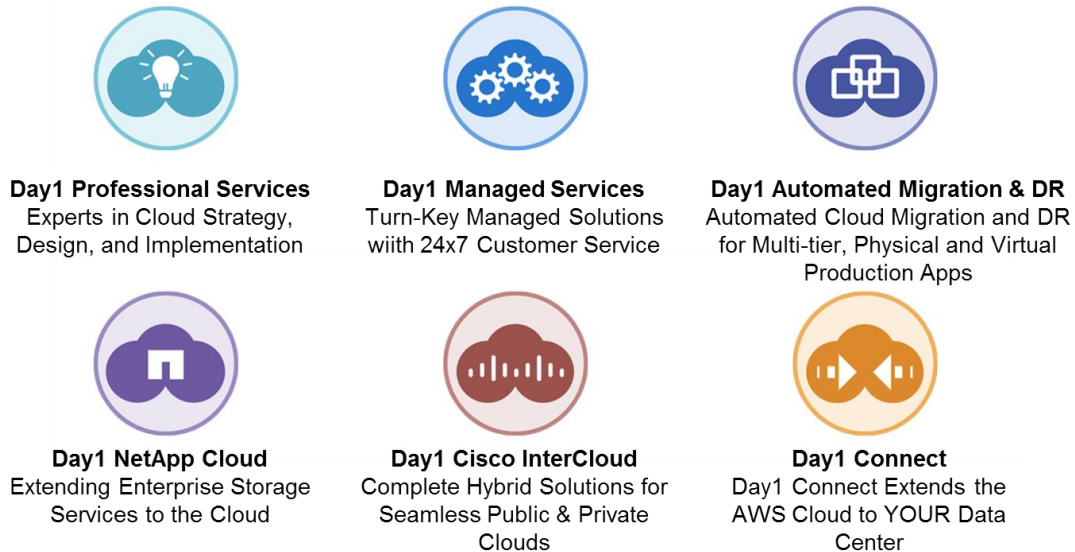


Figure 3: Day1 Lines of Business and Products

Our approach is to be the primary reseller of AWS products and services to NASPO and its customers. We understand that NASPO requires direct access to AWS specific resources and we offer our ability to provide NASPO with the following benefits:

- Our costs are transparent to the end-customer
- AWS price reductions are passed directly to customers immediately
- AWS pricing changes and pass through discounts are in direct control of Day1
- Our immediate access to AWS products ensures that NASPO eliminates delays in obtaining AWS services
- Our use of a master account provides transparent, comprehensive, and consolidated billing
- Our portals provide comprehensive usage reporting and dashboarding

### 1.1.2 NIST Characteristics [RFP 8.1.2]

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

Day1 understands the need for NASPO and all NASPO purchasing entities to have the ability to obtain cloud based solutions that meet NIST essential characteristics as it provides an industry accepted baseline for cloud based services. For the following sections below, Day1 has provided NASPO with a highlight of our understanding of each NIST characteristic, in addition to an explanation of how our solution satisfies the NIST characteristics. Day1's offering of AWS is NIST compliant as 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). AWS has leveraged federal security personnel with developing 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).

### 1.1.2.1 On-Demand Self-Service [RFP 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.*

**Our Understanding:** NIST characterizes On-Demand Self-Service as the ability for consumers to unilaterally and automatically provision computing capabilities to include server time and network storage without manual intervention for each service. Day1 understands that self-service of IT resources is a compelling reason to leverage the cloud as it allows organizations to quickly provision IT resources without creating further deployment delays as characterized by an exhaustive procurement cycle.

**How Day1's Cloud Solutions Satisfies NIST Characteristic and Capability:** Day1 asserts that AWS provides NASPO with the ability to meet these requirements as AWS provides consumers of all sizes with on-demand access to a wide range of cloud infrastructure services.

**How Self-Service Technical Capability Is Met:** Day1 will provide NASPO with the ability to leverage on-demand self-service to provision servers, storage, networking components, and bandwidth through the use of AWS Identity and Access Management (IAM). Additionally, the AWS Management console can be used by NASPO staff to access and manage AWS resources through a simple and intuitive web-based user interface secured through Secure Socket Layers (SSL) encryption. Day1 staff has deep experience with the different services available on AWS through a combination of proven methodologies from previous engagements with customers, strong industry knowledge, understanding best practices, and constant organizational obligations for continued technical training. AWS specific offerings include global compute, storage, database, analytics, application, and deployment services. *Figure 4: AWS Services and Descriptions* below is a high level description of the AWS cloud platform categories that Day1 can bring immediately to NASPO.

#### EXPERIENCES WITH AWS

In support of Georgetown University, our consulting services developed a cloud adoption lifecycle to include Discovery, Planning, Assessment, Migration, Stabilization, Operation, and Optimization. During the Discovery and Planning for a migration into AWS, our consulting team leveraged the Cloud Adoption Framework from AWS to build a common understanding and baseline across teams, and the grounding of the migration plan. As part of the Migration and Stabilization phases, our team provides Georgetown University with a diverse array of AWS products and offerings to ensure self-service and provisioning of cloud services.

<b>DEPLOYMENT &amp; MANAGEMENT</b>		<b>SECURITY &amp; ADMINISTRATION</b>	
Services to help with management of credentials for access to AWS services, to monitor NASPO customer applications, to create and update stacks of AWS resource, deploy applications, use hardware security modules (HSMs) and log AWS API activity.		Services to help facilitate the security and administration of NASPO customer resources deployed in the AWS cloud. Implement controls to ensure an optimized shared security model.	
<b>APPLICATION</b>		<b>MOBILE SERVICES</b>	
A variety of managed services to use with organizational applications including services that provide application streaming, queuing, push notification, email delivery, and transcoding.		Unique services that facilitate and enable the development of mobile centric applications. Deploy, analyze, and test across multiple platforms.	
<b>DATABASE</b>	<b>ANALYTICS</b>	<b>ENTERPRISE APPLICATIONS</b>	
Fully managed relational and NoSQL database service, in-memory caching as a service and petabyte-scale data-warehouse service.	Cloud based analytics services to process and analyze any volume of data, whether it by managed Hadoop clusters, real-time streaming data, petabyte scale data warehousing, or orchestration.	A wide variety of enterprise level applications that provide NASPO customer with office automation capabilities.	
<b>NETWORKING</b>	<b>COMPUTE</b>	<b>STORAGE</b>	
A full range of networking services including logically isolated networks, private network connection to the AWS cloud, and highly available and saleable DNS service and deliver content to end users.	A wide selection of compute instances which can scale up and down automatically to meet the needs of NASPO customer applications, a managed load balancing service as well as fully managed desktops in the cloud.	Low-cost data storage with high durability and availability. AWS offers storage choices for backup, archiving, and disaster recovery, as well as block, file, and object storage.	
<b>AWS GLOBAL INFRASTRUCTURE</b>			

Figure 4: AWS Services and Descriptions

AWS has a comprehensive catalog of products that are used to provide the services mentioned in Figure 4 above. As an AWS reseller, Day1 will provide NASPO with direct access to these products and services without the complications of billing, transfer of services, and delay in purchasing or obtaining these services through a separate reseller. A sampling of the specific AWS technologies, and products that can be directly purchased through Day1, can be found in Figure 5: AWS Specific Technologies and Services below:




















































MANAGEMENT TOOLS	SECURITY & IDENTITY	DEVELOPER TOOLS
 CloudWatch  CloudFormation  CloudTrail  Config  OpsWorks  Service Catalog  Trusted Advisor	 Identity & Access Management  Directory Service  Malicious Web Traffic (WAF)  Certificate Manager	 CodeCommit  CodeDeploy  CodePipeline
APPLICATION SERVICES		MOBILE SERVICES
 API Gateway  AppStream  CloudSearch	 Elastic Transcoder  Simple Email Service (SES)  Simple Queue Service (SQS)  Simple Workflow Service (SWF)	 Mobile Hub  Cognito  Device Farm  Mobile Analytics  Simple Notification Service (SNS)
DATABASE	ANALYTICS	ENTERPRISE APPLICATIONS
 Relational Database Service (RDS)  DynamoDB  ElastiCache  Redshift  Database Migration Service	 Managed Hadoop Framework (EMR)  Data Pipeline  Elasticsearch Service  Kinesis  Machine Learning	 WorkSpaces  WorkDocs  WorkMail
NETWORK	COMPUTE	STORAGE
 Virtual Private Cloud (VPC)  Direct Connect  Route 53	 Elastic Cloud Compute (EC2)  EC2 Container Service  Elastic Beanstalk  Lambda	 Simple Storage Service (S3)  CloudFront  Glacier  Import/Export Snowball  Storage Gateway

Figure 5: AWS Specific Technologies and Services

### 1.1.2.2 Broad Network Access [RFP 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.*

**Our Understanding:** NIST characteristics of Broad Network Access require that services are available over a network and accessed through standard mechanisms that encourage the use of heterogeneous platforms. Day1 understands that this independence from geography and deployment of services that are easily network accessible provides NASPO purchasing entities with great flexibility in deploying, connecting, and accessing IT resources.

#### How Day1’s Cloud Solutions Satisfies NIST

**Characteristic and Capability:** Day1 affirms that AWS complies with these characteristics as they provide a simple way to access servers, storage, databases, and a broad set of application services over the Internet through the AWS Management Console which will provide NASPO with the ability to provision services needed by each purchasing entity via a web application, mobile client, command line access through Secure Shell (SSH) or programmatically through published and well documented Application Program Interfaces (APIs). Additionally, AWS owns and maintains the network-connected hardware required for these application services. The table below provides a list of applicable web browsers that NASPO may use to access AWS provisioned resources:

**EXPERIENCES WITH AWS**

The Millennium Challenge Corporation (MCC) currently operates headquarters in Washington, DC while it maintains its IT resources in hybrid solution of on-premise IT and AWS. Additionally, staff of MCC often work from home or at remote offices. Our team’s use of AWS allows for broad network access of resources and allows the organization to be independent of geography.

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

Figure 6: AWS Browser Compatibility

### 1.1.2.3 Resources Pooling [RFP 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.*

**Our Understanding:** The main NIST characteristics of Resources Pooling require that “the provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand”. Day1 understands the significance

of resource pooling to NASPO purchasing entities as it ensures greater efficiency in IT services and provides for economies of scale in pricing.

**How Day1’s Cloud Solutions Satisfies NIST**

**Characteristic and Capability:** Day1 is highly experienced in developing and architecting diverse cloud models and can provide NASPO customers with the ability to implement cloud models that provide resource pooling abilities based on the requirements of the customer. Leveraging AWS we can provide NASPO with a virtualized, multi-tenant environment that can be used by NASPO purchasing entities to support multiple cloud deployment models with specific resource pooling requirements that meet Public, Community, Hybrid, and Private requirements. 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.

**EXPERIENCES WITH AWS**

Day1 is currently a cloud service provider to the United States Census Bureau where we provide the organization the ability to develop public, community, hybrid or private cloud solutions to affiliated agencies in an effort to see greater resource pooling and cost efficiencies.

Additionally, Day1 has the ability to provide government customers with access to AWS GovCloud which is a community cloud designed to allow US government agencies and customers the ability to move sensitive workloads into the cloud by addressing specific regulatory and compliance requirements. The AWS GovCloud framework adheres to U.S. International Traffic in Arms Regulations (ITAR).

**1.1.2.4 Rapid Elasticity [RFP 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.*

**Our Understanding:** The NIST requirements for Rapid Elasticity state that resources should be provisioned and released elastically and may also require for automated scalability to meet rapid outward and inward demands. Day1 understands that the majority of cloud adopters seek the rapid elasticity afforded through the cloud as it allows organizations to quickly scale up (or down) resources based on demand.

**How Day1’s Cloud Solutions Satisfies NIST Characteristic and Capability:** AWS provides a massive global cloud infrastructure that allows for quick innovation, experimentation, and iteration of services through elasticity in services and capabilities. Traditional on-premise IT service models require weeks or months for hardware procurement and deployments that through AWS can be instantly deployed and can instantly scale up and down as workloads ebb and flow. AWS compute services, such as Elastic Cloud Compute (EC2), will provide NASPO with a cloud solution that is both flexible and allows for NASPO to scale its applications based on its evolving demand for compute. Elastic Load Balancing (ELB) and Auto Scaling can automatically scale a NASPO customer’s AWS resources up to meet unexpected demand and then scale those resources down as demand decreases.

Day1 proposes the use of ELB to provide automated application load distribution for incoming traffic across multiple Amazon EC2 instances. By using ELB, Day1 can help NASPO to achieve a high level of fault tolerance in applications, as the service seamlessly distributes workloads and load capacity in response to incoming application traffic. An additional fault tolerance capability that ELB provides is the ability to detect unhealthy EC2 instances for automatic rerouting of traffic to healthy instances. This automated rerouting can exist for extended periods of time and provide the ability for the unhealthy instances to be restored. Depending on the availability needs of NASPO applications, Team Day1 can help to design EC2 instances and ELB architecture to be enabled within a single Availability Zone (AZ) or across multiple zones for even more consistent application performance.

Day1 can work with NASPO purchasing entities to enable Auto Scaling services to allow for automated resource scaling of Amazon EC2 instances. As part of our services, we can help to capacity plan EC2 instances and define the conditions that trigger the Auto Scaling services, allowing instances to move up or down in capacity according to conditions that we help NASPO customers define. Auto Scaling enables NASPO purchasing entities to closely follow the demand curve for applications, reducing the need to provision Amazon EC2 capacity in advance.

#### 1.1.2.5 Measured Services [RFP 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.*

**Our Understanding:** NIST requires that cloud systems allow for resource control and optimization through metering capabilities similar to a pay-per-use or charge-per-use basis. Day1 understands the importance of measured services to adequately forecast spend and allow for purchasing entities to control use of IT resources. Day1 will utilize AWS automated monitoring systems to provide a high level of service performance and availability.

**How Day1's Cloud Solutions Satisfies NIST Characteristic and Capability:** Day1 will leverage proactive monitoring is 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 to ensure personnel are always

#### EXPERIENCES WITH AWS

In support of University Maryland University College (UMUC), Day1 provides the organization with the flexibility to rapidly scale IT infrastructure based on the demand of compute required to during enrollment periods. This allows for quick expansion during course election and tuition payments and significant cost savings through scaling down during seasonal breaks.

#### EXPERIENCES WITH AWS

Day1 provides Cloud and IT project management support at the Federal Communications Commission (FCC). Our support at the FCC includes consolidation of multiple billing accounts and allowing access to full pay-per-use catalog of multiple cloud providers. This model allows for the FCC to quickly forecast IT spend on a monthly basis and control virtual machine sprawl.

available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

AWS enables NASPO customers to eliminate the need for costly hardware and the administrative struggles that accompany management of on-premise systems. Instead of the weeks and months it takes to plan, budget, procure, set up, deploy, operate, and hire for a new project, Day1 can support NASPO customer's deployment of an AWS environment for immediate deployment in the cloud with unprecedented deployment capabilities from 1, 10, 100, or 1,000 servers. Additionally, Day1's proposed implementation of AWS provides NASPO the ability to utilize a combination of purchasing models to immediately procure and implement cloud compute instances. These purchasing models can be manipulated and optimized to ensure increased cost efficiencies for NASPO purchasing entities and provide greater insight into measured services. The purchasing models include On-Demand, Reserved, Dedicated, and Spot Instances for true flexibility in terms of cost projections and management:

- On-Demand Instances allow NASPO customers to pay a fixed rate by the hour with no commitment;
- Reserved Instances provide NASPO customers with a capacity reservation, and offer a significant discount on the hourly charge for an instance;
- Dedicated Instances allow NASPO customers to pay for compute instances launched on hardware specifically provisioned for NASPO;
- Spot Instances enable NASPO customers to bid whatever price NASPO wants to pay for instance capacity providing for even greater savings if NASPO customers applications have flexible start and end times.

### 1.1.3 Subcategory(ies) [RFP 8.1.3]

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

In addition to providing AWS IaaS solutions, Day1 can provide an array of PaaS, and SaaS solutions through the AWS Marketplace. As a certified *AWS Marketplace Reseller* and *AWS Marketplace Consulting Partner*, Day1 can provide direct access to the expansive Marketplace PaaS and SaaS Service Catalog and provide consulting services to ensure proper implementation of these PaaS and SaaS products. AWS Marketplace is an online software store that helps customers find, buy, and immediately start using software across all different industries that run on the AWS cloud. It includes software from trusted vendors like SAP, Microsoft, and IBM, as well as many widely used open source offerings including WordPress, Drupal, and MediaWiki.

Day1 works very closely with the AWS Marketplace product team, and Day1 is developing unique capabilities that may include in the future private marketplaces for the NASPO ValuePoint customers. This concept of private community marketplaces is an emerging trend that we see as being highly adopted, and our own specialized experience in the Intelligence Community with the CIA sponsored AWS C2S Marketplace gives us a great advantage in deploying this type of model, to include the security and compliance needs of government. IT service catalogs are a great first step in this direction, made available by AWS and many other 3rd party applications, which differ based on the unique needs of each entire enterprise environment. Today we currently offer AWS Marketplace to our WSCA cloud customers, which has been key to our success as an AWS Marketplace partner. Some key benefits to Marketplace include:

- AWS Marketplace offers more than 2,300 software products in 35 categories that customers can launch on AWS with one click.
- For software companies interested in making their products available to AWS customers, AWS Marketplace provides an easy ramp to the Cloud.
- Customers run over 143 million hours a month of Amazon EC2 for AWS Marketplace products.
- AWS Marketplace offers free trials and hourly and monthly pricing models. Customers can get started with software free trials or AWS Free Tier Eligible Software.

Day1 is one of the few premier partners that have been carefully selected by AWS to participate in a pilot program for reselling AWS Marketplace software solutions, designated as an *AWS Marketplace Reseller*. Day1 is an inaugural participant in this program which commenced January of 2016. We were selected by AWS because our Channel Reseller Program performance and ongoing AWS Marketplace sales activity through our WSCA PCHS MA265 contract vehicle.

Day1 Solutions has also been selected by several software vendors who participate in AWS Marketplace, to provide their customers with guidance and integration, designated as an *AWS Marketplace Consulting Partner*. We have an established engagement history working with the technology vendors outside of AWS Marketplace, many of them as legacy vendors with our customers. It is because of our proven ability to help the technology vendor's customers move from legacy systems specifically to the AWS cloud that has gained us this recognition.

Day1 is currently listed as a preferred AWS Marketplace Reseller and AWS Marketplace Consulting Partner for the following software technology product vendors in which we specialize and offer solutions:

- Cisco (networking)
- Sophos (security)
- Trend Micro (security)
- N2W (storage)
- SoftNAS (storage)
- NetApp (storage)
- Splunk (security)
- Marklogic (database)
- MapR (GIS/BI)
- Data Resolution (SharePoint)

**Day1's SaaS offering with Infor:** Infor provides SaaS offerings for several verticals, including Aerospace, Automotive, Distribution, Facilities Management, Fashion, Financial Management, Food and Beverage, Healthcare, Hospitality, Industrial Manufacturing, and the category proposed herein, Public Sector.

#### 1.1.4 Compliance with Attachments C & D [RFP 8.1.4]

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

As stated in sections 1.1.1 *Cloud Services Model(s) and Deployment Model(s)* and 1.1.2 *NIST Characteristics [RFP 8.1.2]* Day1 understands the importance of complying with NIST characteristics and having a diverse service and deployment model to meeting the unique requirements of each NASPO purchasing entity. Day1 certifies that it will provide solutions that comply with the requirements of Attachments C & D. Please refer to sections 1.1.1 *Cloud Services Model(s) and Deployment Model(s)* and 1.1.2 *NIST Characteristics [RFP 8.1.2]* for more information.



### 1.1.5 Adherence to Services, Definitions and Deployment Models in Attachment D [RFP 8.1.5]

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

As stated in section 1.1.1 *Cloud Services Model(s) and Deployment Model(s)* Day1 stands ready to provide NASPO purchasing entities with cloud based service offerings through AWS. Day1 has extensive experience customizing cloud architectures for state, local, federal governments and enterprises that adhere to the services, definitions, and deployment models identified in the Scope of Services in Attachment D. Please refer to sections 1.1.1 *Cloud Services Model(s) and Deployment Model(s)* and 1.1.2 *NIST Characteristics [RFP 8.1.2]* for more information.

## 1.2 (E) Subcontractors [RFP 8.2]

### 1.2.1 Direct Delivery or Subcontractors [RFP 8.2.1]

*Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.*

Day1 has several key employees, including executive level staff members, who have previously worked at AWS and have extensive experiences providing cloud management services to NASPO. Day1's CEO and Founder, Mr. Luis Benavides, previously served as a Principal Sales Executive at AWS and continuously engages with AWS executive level staff to identify upcoming product offerings and capabilities prior to release. Our Contract Manager for WSCA, Mr. Sean Wilson, currently manages all work under our NASPO WSCA vehicle and continues to build our services around NASPO customer needs. These leaders help to shape our Professional and Consulting Services arms as they have a comprehensive understanding as to how our organization can expeditiously bring new services to NASPO. Together, these revolutionary leaders have been involved in the cloud space and with AWS and WSCA from its infancy and played active roles in its evolution. They bring an unprecedented connection and bond to AWS and WSCA, and will make their relationships directly available to NASPO. Our comprehensive organizational capabilities and our strong leadership team provide NASPO with unique value-added services. Some of the main advantages Day1 brings include:

	The Competition	Benefits of Day1 to NASPO
<b>Purpose-built vs Piece Mailed Solution</b>	Most of Day1 competitors in the space will piece mail a solution to meet the requirements NASPO's solicitation. This includes piece mailing team members for: AWS resale for selling the services, systems integrator to implement, and managed service provider (MSP) for operations & maintenance (O&M).	Day1 provides the team with a purpose-built from the ground up to be an end-to-end solutions provider of value added reseller (VAR) for AWS resale; advanced consulting partner for systems integration; and managed service provider for O&M. We help NASPO remove any issues and/or concerns surrounding the capability of specific team members to deliver on AWS.

The Competition		Benefits of Day1 to NASPO
<b>Past Performances with Cloud and NASPO</b>	Most vendors will require multiple companies to serve either meet the past performance requirements and technical requirements of the solicitation.	Day1 provides the team with comprehensive past performance experiences in technical delivery, NASPO contract management, and work with participating entities. Day1 has developed an extensive network of customers within NASPO and continues to add to our past performance through the existing WSCA contract. We have more existing Purchasing Addendums (14 different PAs) than any other prime on the current NASPO WSCA vehicle with.
<b>Siloed vs Integrated Solutions</b>	Other offerors who respond to this solicitation will try to integrate a siloed solution and are unlikely to have completely worked as a team at the capacity in which NASPO requires. They do not have a great level of maturity, understanding, and familiarity with each other's disparate organizational processes. Their strategies often include attempting to integrate companies with siloed capabilities and solutions offerings.	As a single company, Day1 provides NASPO with a completely integrated solution. While many offerors provide siloed team members with AWS partnership credentials, we provide NASPO with an independently audited, approved, and AWS certified end-to-end solutions offering. Day1 independently offers the comprehensive solutions that other offerors have attempted to integrate.
<b>Service Level Agreements (SLA)s and accountability</b>	Offerors with multiple teaming partners will be required to pass-through SLA's management, negotiation, and changes as it requires complete buy-in from multiple parties. Additionally, accountability and financial considerations for these SLAs are not specifically within the control of NASPO as they are provided to the prime.	Day1 provides NASPO with direct access to all SLA's from AWS procurement, implementation to management. NASPO considerations and changes to SLAs are performed directly with Day1 without the requirement to involve teaming partners. Day1 does not require the pass-through of SLA's and can be held accountable for all SLA's.
<b>Pricing pass-through</b>	Due to the fact that most offerors may require teaming partners to perform this work...pricing changes, mark-ups, and discounts are an outcome of negotiation efforts across the team. NASPO does not have transparency into these efforts in a prime/sub relationship.	As a single entity providing services, there is no need for Day1 to negotiate pricing and possible pass-through discounts. NASPO can have these types of discussions directly with Day1 without the need to include other partners and/or subs; thus mitigating potential conflict, cost escalations, etc.

Figure 7: Benefits of Day1 to NASPO

**Day1's SaaS offering with Infor:** Infor provides our SaaS services primarily with Infor staff. We have partnered with Amazon Web Services (AWS) to provide IaaS services and with Day1Solutions to support customer implementations, transitions and migrations. Both subcontractors have been determined to be highly qualified in provide the requisite services. AWS has been supporting Infor for over 10 years and Day1Solutions is a current WSCA prime.

### 1.2.2 Subcontractor Usage [RFP 8.2.2]

*Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.*

Day1 is a current contract holder of WSCA and is currently authorized to provide services to NASPO and purchasing entities. Day1 will be our teaming partner Infor as a Subcontractor to provide additional bench strength (with over 12,00 employees) and PaaS/SaaS specific skillsets on the NASPO ValuePoint Master Agreement for Cloud Solutions. As an existing prime contract holder for the existing WSCA vehicle, Day1's extensive knowledge with the contract will prove to be vital to the successful transition and continued operation of the NASPO ValuePoint Master Agreement. Day1's discrete knowledge of existing WSCA customers will allow us to stay engaged as we bring on any subcontractors. Additionally, Day1's specific experiences with existing purchasing entities, and participating states allows for even greater understanding of work at the task order level. Additionally, Day1 can use the large global presence of Infor to ensure program delivery with over 147 locations.

Day1 has the current staff, experience, and capability to manage all subcontractor work under the contract. As a prime on NASPO WSCA, Day1 employs the use of subcontractors on a limited basis. This is often the case when there are unique requirements in a task order and a niche subcontractor can be leveraged to help expedite an effective delivery. Day1 will use the same approach on work going forward on the NASPO ValuePoint Master Agreement for Cloud Solutions.

### 1.2.3 Subcontractor Qualifications [RFP 8.2.3]

*If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.*

Day1 is highly selective in selecting our subcontractors and teaming partners. Our qualifications for selection and evaluation of subcontractors include: long-term stability, financial strength, history of customer satisfaction, technical excellence, complementary skills, culture, business practices, and demonstrated commitment to customer success. Day1 will continuously evaluate potential subcontractors to be responsive to NASPO's existing and evolving needs throughout the term of the contract. Immix maintains a database of pre-screened and approved subcontractors consisting of proven small and large IT products, services and solution based companies. Potential subcontractors with NASPO and/or cloud-centric experience and expertise are identified by Day1's NASPO contract manager. Subcontractors are evaluated based on their ability to provide services described in the NASPO ValuePoint Master Agreement for Cloud Solutions. Criteria for subcontractor selection are designed to optimize the relationship for the long-term and include:

- Cloud domain-specific capabilities to support the existing and future requirements of the NASPO
- Demonstrated ability to perform in specific NASPO task areas to include IaaS, SaaS and PaaS

- Strong past performance record, with emphasis on diverse enterprise level customers
- Proven record of service excellence (both technical expertise and quality management) in support of complex, multidisciplinary and geographically dispersed task orders
- Demonstrated access to resources qualified and available to support multiple task order requirements
- Competitive employee benefits to attract and retain proven performers
- Certifications within their core competencies

Day1 has selected our teaming partner, Infor, based on the strict qualifications stated above as well as their ability to meet the mandatory requirements of the solicitation and bring extensive value added capabilities with AWS based PaaS and SaaS products. Infor is the world's third largest provider of enterprise software, with approximately \$2.8 billion in revenue and is one of the fastest growing business software providers, with more customers than their next two largest competitors combined. Infor's solutions highly compliment Day1 as their products are built on AWS and inherit the security and technical standards of the platform. Additionally, their large customer footprint is vital to expanding Day1's ability to growing business on NASPO WSCA. Their representative accounts are as follows:

- State of Michigan
- State of Arizona
- State of New Hampshire
- City of San Francisco
- University of California
- State of South Dakota
- City of Chicago
- School District of Hillsborough County
- San Antonio Water System
- New York City
- Albuquerque Public Schools
- Fairfax County Public Schools
- University of North Carolina
- City of Houston
- Louisville and Jefferson County MSD
- Miami Dade County
- City of Las Vegas
- Memphis City Schools
- Atlanta Independent School System
- Los Angeles County Metropolitan Transportation Authority
- City of Dallas
- Southern Maryland Electric
- Chicago Transit Authority
- Denver Public Schools
- City of Atlanta
- U.S. House of Representatives
- FBI

### 1.3 (E) Working with Purchasing Entities [RFP 8.3]

---

#### 1.3.1 Working with Purchasing Entities through Data Breaches [RFP 8.3.1]

---

Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as: Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved; Response times; Processes and timelines; Methods of communication and assistance; and Other information vital to understanding the service you provide.

Our ValuePoint Contract Administrator, Mr. Sean Wilson, has full autonomy of the contract and will serve as the single point of contact for our contract and will support all collaboration efforts with Purchasing entities. Mr. Wilson currently serves as the Day1 NASPO WSCA Contract Manager and has first-hand experience working with Purchasing Entities. *Figure 13: Day1's Customer Service and Communication Structure* below shows how different personnel are involved with Purchasing Entities and their roles throughout the process. During the participating addendum period, entities can select and define varying levels of dedicated service (to be defined based on our managed services

agreements) that allow for online self-help, online support and telephone based Help Desk services, real-time case management, or contracted custom support services. We offer NASPO and Purchasing Entities with multiple methods of communication should they encounter a data breach and need to interface with Day1:

- Direct customer interface at the program, contract, Purchasing Entity, and task order levels
- Dedicated Contract Administrator/Manager, Mr. Sean Wilson with incumbent knowledge of NASPO WSCA customer service requirements
- 24x7 technical support and on-call support desk for issues that require immediate resolution from our managed services team
- Online self-service for issues that need attention through our [www.Day1Solutions.com/NASPO](http://www.Day1Solutions.com/NASPO) landing page at [www.Day1Solutions.com/NASPO](http://www.Day1Solutions.com/NASPO)
- Email group for bulk requests at [NASPO@Day1Solutions.com](mailto:NASPO@Day1Solutions.com)

**EXPERIENCE WITH PURCHASING ENTITIES**

With the largest number of Participating Addenda out of any prime vendor, Day1 is authorized to work with agencies in 14 states and as of time of submission is working with states such as Florida and North Dakota.

Purchasing Entities will be able to monitor in real time their customer service cases from initiation to close out through the customer service portal. If a breach is identified by a purchasing entity, the entity may request support through our online portal. As seen in Figure 8 below, the major elements of our case management system from request through close out is repeated as necessary until the data breach is resolved to their satisfaction. Our Customer Support staff and management team will rely on our many years of providing similar customer support services for other clients as well as industry standards and best practices for case and service management including, but not limited to, the IT Infrastructure Library, or ITIL.

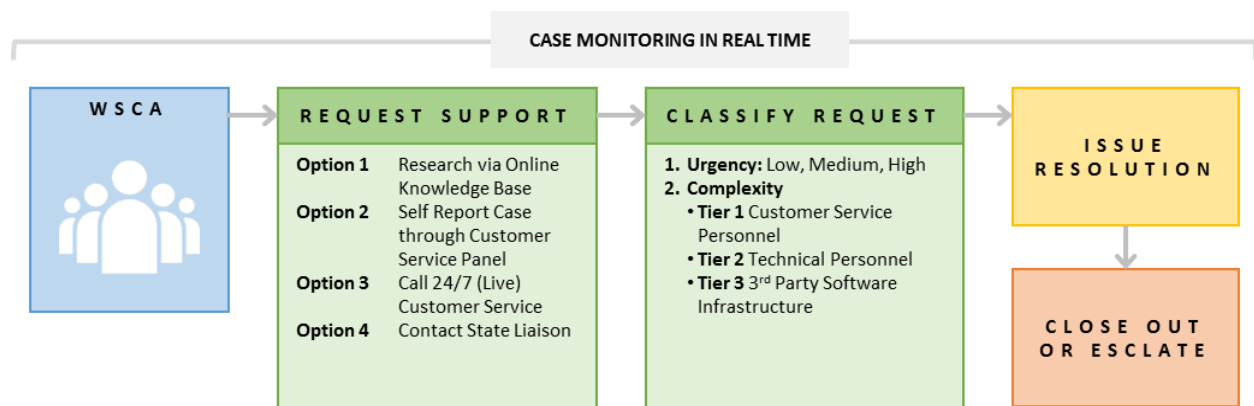


Figure 8: Day1's Case Management Approach

Additionally, 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 AWS three-phased approach that Day1 can use to help 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 through AWS support. 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.

**Day1's SaaS offering with Infor:** Infor's Security Incident procedure follows a similar process as other Cloud Support incidents. However, the basic process appears below.

1. Incident creation and logging in our system
2. Determination of the type and severity of incident that has occurred
3. Escalation as necessary
4. Investigation with Impact Assessment
5. Documentation of events
6. Incident containment
7. Gathering of evidence
8. Notification of affected customers, insurance carriers, third party providers, and/or law enforcement
9. Removal and recovery (e.g., malware)
10. Post-mortem study

Infor notifies affected customers of a confirmed breach involving their data as quickly as reasonably possible, typically within 48 hours of confirmation of such a breach.

### 1.3.2 Adware, Software or Marketing [RFP 8.3.2]

---

*Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.*

Day1 asserts that it will not engage in, nor permit agents to push adware, software, or marketing that is not explicitly authorized by NASPO and associated Participating Entities.

### 1.3.3 Test/Staging Environment [RFP 8.3.3]

---

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

Day1 proposes the implementation of Amazon Virtual Private Cloud (VPC) to provide disparate environments for user test/staging environments. Additionally, VPC configurations and the use of CloudFormation templates can be used to keep production VPCs identical to that of test/staging environments. The design, engineering, and implementation of Amazon VPC provides the NASPO customers with isolated hosted server deployments. Amazon VPC includes the following characteristics:

- Provision logically isolated computing/processing resources to host NASPO customer application-hosting environments.
- VPC configurations and CloudFormation templates can be used to ensure environments are identical.
- Controlled access to VPC can help to separate environments and users accessing environments.
- CloudFormation templates can be used to quickly spin up environments.

### 1.3.4 Accessibility [RFP 8.3.4]

---

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

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.

**Day1's SaaS offering with Infor:** Infor has and maintains VPAT certificates for each product in our recommended solution. Infor recognizes the inherent value and importance of making its software applications operable for individuals with varying degrees of physical impairment – regardless of whether the impairment is visual, auditory, or manual movement. In support of Section 508 of the Amended Rehabilitation Act of 1998 as implemented by

Chapter 36 of the Code of Federal Regulations Part 1194 (36 CFR 1194), Infor has made and is continuing to make measurable strides in its software design to adopt accessibility-friendly features into its product offerings. Such measures can include – but are not limited to:

- Product project planning that considers accessibility implications for each product release
- Coding efforts to offer alternative text presentations of graphical displays
- Goals to ensure that Infor products are compatible with existing Assistive Technology (including Microsoft Windows Accessibility and Oracle JAWS)
- Deliberate elimination of former color-coding of fields that impeded system operation by individuals with color-perception impairment
- Deliberate assurance that Infor products operate without the use of audio prompts and signals
- Conscious inclusion of parallel methodologies so that any Infor application user can execute desired operations using mouse, keyboard, or both
- Completed the Voluntary Product Accessibility Template provided by the Information Technology Industrial Council (ITIC) in order to more accurately identify areas for potential improvement with respect to accessibility issues

### 1.3.5 Web Browsers [RFP 8.3.5]

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

As described in *Section 1.1.2.2 Broad Network Access [RFP 8.1.2.2]* Day1 asserts that AWS resources are readily accessible through multiple methods to include CLI, mobile, and through the web. The table below provides a list of applicable web browsers that NASPO customers may use to access AWS provisioned resources:

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

Figure 9: AWS Browser Compatibility

**Day1's SaaS offering with Infor:** Infor CloudSuite Public Sector supports the following browsers: Internet Explorer 9.0 (32-bit version) Internet Explorer 10.0 (32 and 64-bitversions), Internet Explorer 11.0 (32 and 64-bit versions), Mozilla Firefox34 for Windows, Google Chrome 39 for Windows, and Safari 7.1 for Mac OS



### 1.3.6 Meeting Purchasing Entities [RFP 8.3.6]

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

As an existing prime on the WSCA Public Cloud Hosting contract Day1 currently utilizes the WSCA contract to promote cloud adoption at the enterprise level in government agencies educational institutes nationwide. With the largest number of Participating Addenda out of any prime vendor, Day1 is authorized to work with agencies in 14 states and is currently engaged with a number of others to help them realize the benefits of cooperative purchasing. We have proven the ability to meet with Purchasing Entities and establish a report prior execution of Service Level Agreement (SLA). Prior to execution of a SLA Day1 works the Purchasing Entity to perform a kickoff meeting. The objective of our kickoff meetings include:

- Introduction of team members, and points of contact with key stakeholders
- Establishing expectations and refining scope of effort
- Defining roles and responsibilities for each effort
- Highlighting critical timelines, tasks, milestones, or events

During the time of the release of this solicitation and submission of the Day1 proposal, the Day1 team has held three kickoff meetings with Purchasing Entities to include meetings with the State of Florida, Maryland Department of Human Resources, and Minnesota Office of Information Technology.

### 1.3.7 Project Schedule Plans [RFP 8.3.7]

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

The development of project schedule plans or work plans are unique to each solution and Day1 will work with each Participating Entity to tailor a plan based on the objectives of the project. Day1 understands the details required in project schedules can grow exponentially based on factors such as system size, complexity of environment, security posture, etc., and we are prepared to provide consulting services that can customize a plan specific to each Participating Entity. Our approach to customizing and tailoring a project can be found under *Section 1.19.2 Customize and Personalize Solutions [RFP 8.19.2]*.

The figure below is a Sample Work Breakdown Structure (WBS) that was developed by Day1 after multiple data gathering and baselining sessions. As discussed above, the Day1 team works will work with each Participating Entity to clearly define the requirements and objectives of the project and outline possible data gathering techniques. Upon developing our understanding of the environment, Day1 may create a work plan or schedule in the form as a

#### DAY1 PARTICIPATING ADDENDUMS

As listed on the NASPO website Day1 currently has the following PA's to include: Alaska, Arkansas, Colorado, Delaware, Hawaii, Maryland, Minnesota, Montana, South Dakota, Utah, University of Maryland University College. PA's currently being developed and anticipating signature as of submission of this proposal include: Florida and North Dakota.

WBS. Day1 may use common tools such as Microsoft Visio or Excel to develop a WBS as a basis for a work plan and project schedule.

ID	Tasks/Sub-Tasks	Resources	LOE	Software Cost (or N/A)
1001	<b>Requirements</b>			
2025	<b>Design</b>	Tony & Jon		* Assumption bas
2026	<b>Design Shared Infrastructure</b>			
2027	- AWS Account Structure		72	Estimate is 2 FTE to support ~7 AV the production ac
		Sara		Estimate is 2 FTE support ~7 AWS and 1 day for eac environment (dev
2028	- VPC Design		128	Estimate is 2 FTE security tool per t support procurer
		Tony		
2029	- Security Tools			
		Jon		
2030	- Identity Store	Jon		
2031	- Map Security Controls to Identity Store Tool	Jon	16	
2032	- Design identity users, groups, roles, and service accounts	Jon	16	
2033	- Analysis of Alternatives (Identity)	Jon	8	
2034	- Select Identity Store	Jon	8	
2035	- Procure Identity Store	Jon	8	
2036	- SEIM	Jon		
2037	- Designate data sources and formats	Jon	16	
2038	- Validate SEIM requirements	Jon	16	
2039	- Analysis of Alternatives (SEIM)	Jon	16	
2040	- Select SEIM	Jon	8	
2041	- Procure SEIM	Jon	8	
2042	- A/V	Tony		
2043	- Validate A/V requirements	Tony	8	
2044	- Analysis of Alternatives (A/V)	Tony	8	
2045	- Select A/V	Tony	8	
2046	- Procure A/V	Tony	8	

Figure 10: Sample WBS using Visio

Through one of our Project Management Information System (PMIS) tools, MavenLink, our team can create comprehensive WBS and project schedules and share them as Gantt charts to our customers and to NASPO Participating Entities. The figures below show how our team can develop a project plan in MavenLink and share online with our customers who want to collaborate in the process. Our project plans provide our team with a deep understanding of the project schedule, resources, milestones, critical path, and even costs. We will work with each Participating Entity to ensure that our project plans provide the necessary fidelity required to manage each project.

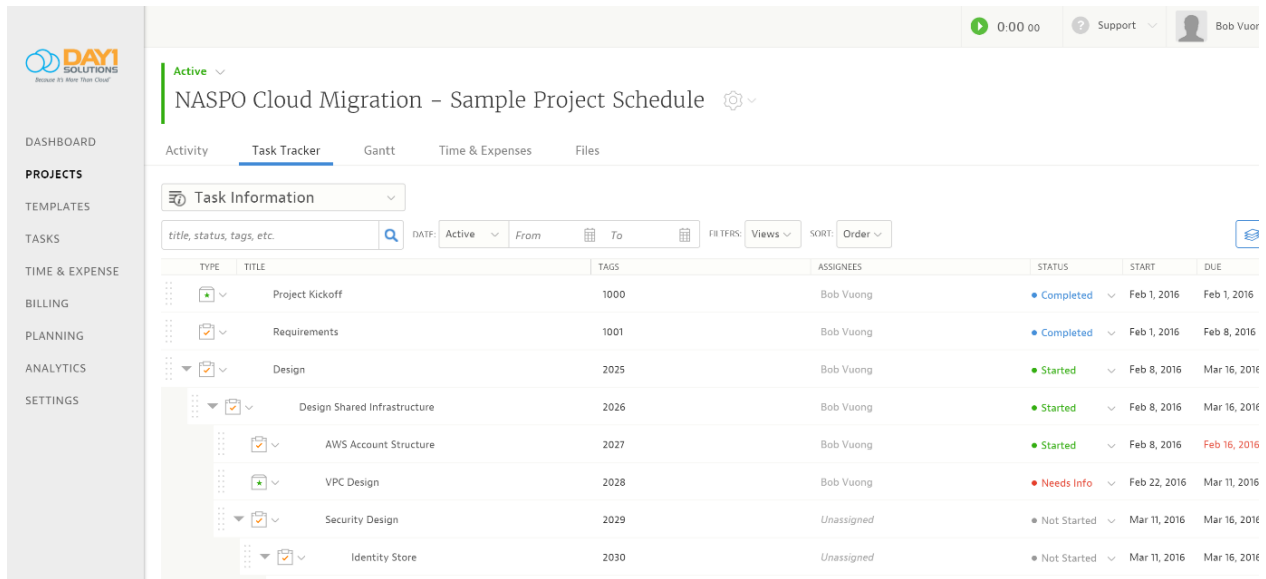


Figure 11: Sample WBS using MavenLink

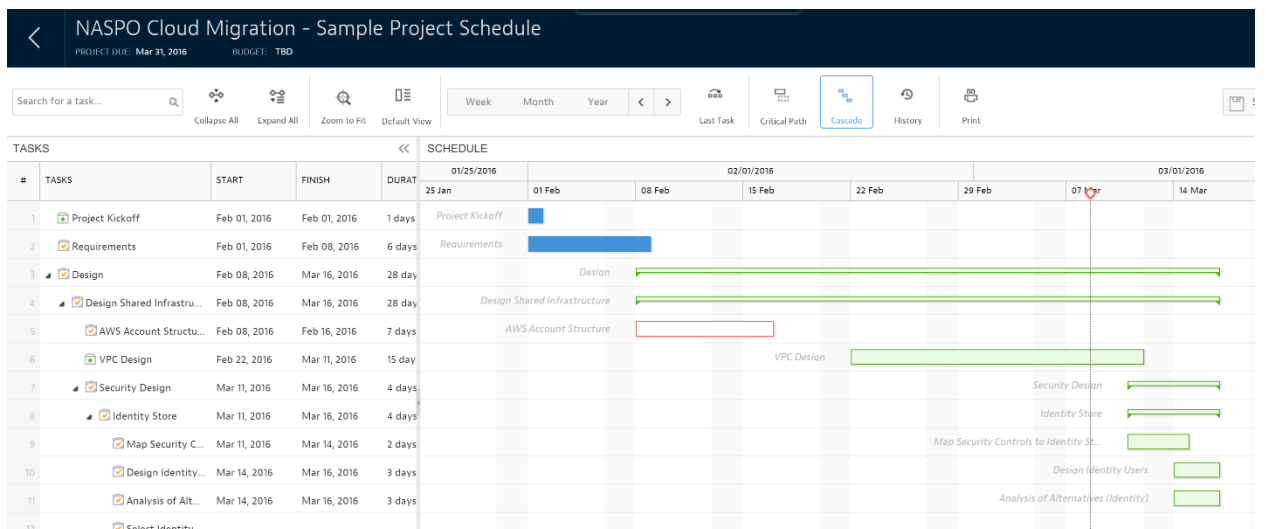


Figure 12: Sample Gantt Chart using MavenLink

## 1.4 (E) Customer Service [RFP 8.4]

Day1’s approach to customer service focuses on the entities individual needs and preferences. As have a strong understanding of customer service as evident with our strong number of Participating Addendums that exist on our current NASPO WSCA contract vehicle. Through our experiences with NASPO WSCA we understand that in order to provide effective customer service, our team must have diverse methods of communication and interaction with NASPO and each NASPO Purchasing Entity. For example, what NASPO expects from our customer service team at the Purchasing Addenda development process may differ greatly from a purchasing entities’ customer service request as a web service is no longer responding.

We offer multiple methods of communication and interactions with our customers as seen in *Section 1.3.1 Working with Purchasing Entities through Data Breaches [RFP 8.3.1]*. Additionally, upon award, we will implement a toll free phone number for direct contact with our organization. During the participating addendum period, entities can select and define varying levels of dedicated service (to be defined based on our managed services agreements) that allow for online self-help, online support and telephone based Help Desk services, real-time case management, or contracted custom support services. We have clear lines of delineation for customer service and communication as seen in *Figure 13: Day1's Customer Service and Communication Structure* below. Our ValuePoint Contract Administrator, Mr. Sean Wilson, has full authority and autonomy of the contract and will serve as the single point of contact for any customer service issues. Should we fail to meet agreed upon incident response times or the problem is not satisfactorily resolved, the user can escalate the problem, first by contacting their state liaison or directly engaging our Contract Administrator/Manager.

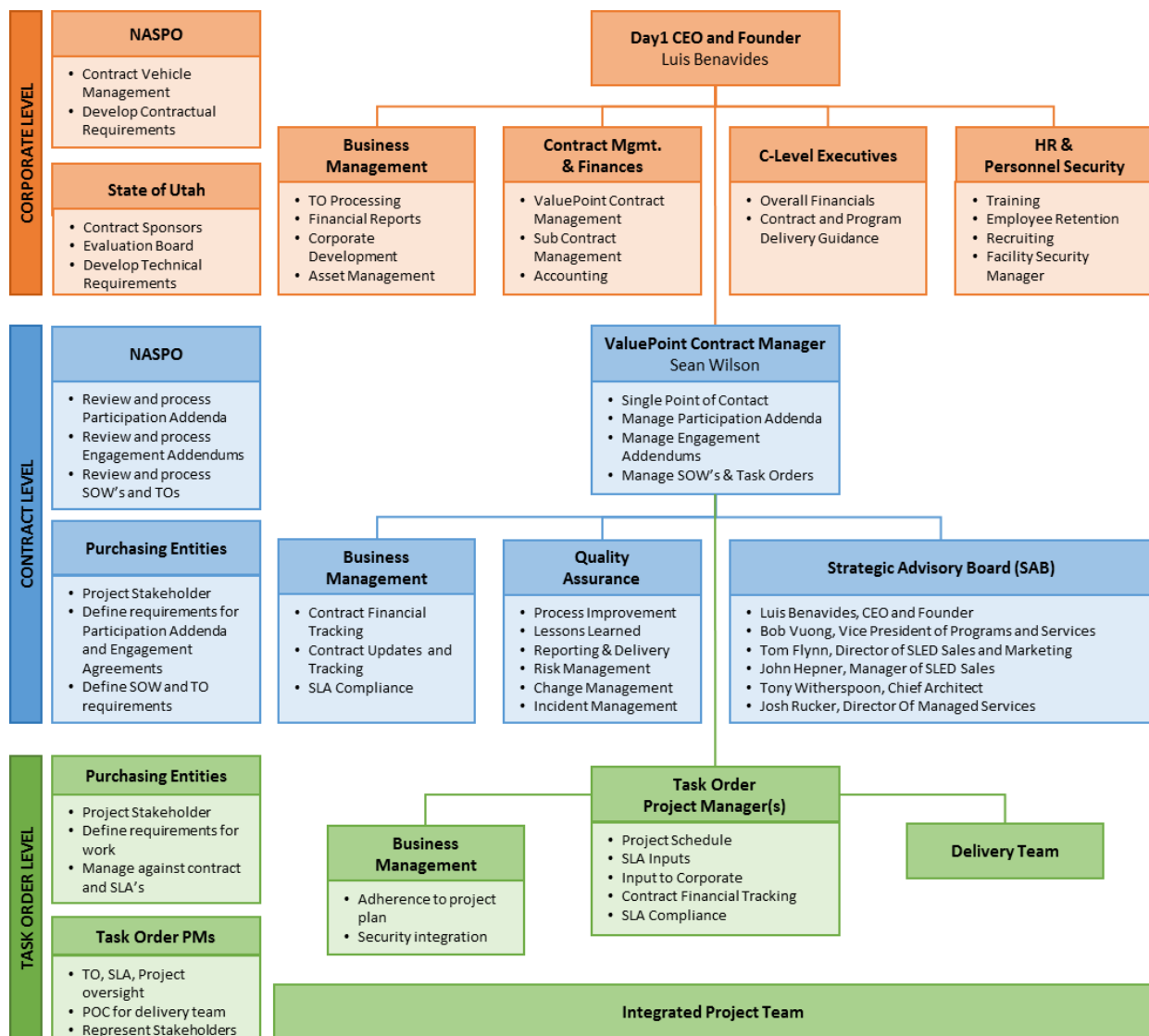


Figure 13: Day1's Customer Service and Communication Structure

Day1 will provide NASPO and Purchasing Entities with the ability to interface entirely online – selecting, purchasing, provisioning, and de-provisioning services; migrating to and from the cloud; and engaging customer support – through the multiple methods described above to include online self-service through our NASPO landing page at [www.day1solutions.com/NASPO](http://www.day1solutions.com/NASPO) or through email group for bulk requests at [NASPO@Day1Solutions.com](mailto:NASPO@Day1Solutions.com). Additionally, we provide Purchasing Entities with the ability to create a case themselves through the customer service portal or they can call our 24/7 live customer support call center to report their problem and have a case created. All new cases are forwarded automatically to Day1's managed services support representative, Contract Administrator/Manager, and the applicable state liaison as well as back to the user for confirmation. We also encourage telephone and face-to-face service requests either through our assigned state liaisons or our 24/7 live customer support call center.

#### 1.4.1 Customer Service [RFP 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).*

Day1's tiered approach to ensuring customer service excellence assigns three areas of management responsibilities and escalation (corporate, contract/program, and TO level), which are color coded in *Figure 13: Day1's Customer Service and Communication Structure*. This tiered approach shows Day1's leadership commitment at each level or the organization and provides some possible escalation scenarios for correlating NASPO leaders on the contract. This structure of the Program Management Office (PMO) is designed with clearly defined lines of escalation, reporting, communication, responsibility and authority and enables proactive management of all activities. Our Contract Manager has the authority to make commitments for Day1 on technical and administrative matters related to this master agreement. Our Day1 Contract Manager will serve as the single point of contact for NASPO and has ultimate responsibility for contract management with support from NASPO. Additionally, the Contract Manager will supervise all staff members supporting both the master agreement and all TOs, overseeing Task Order Project Managers (PM) that provide day-to-day direction Task Lead and TO staff to ensure NASPO customer's satisfaction. Our Contract Manager will incorporate feedback from NASPO and all PMs to ensure that all issues are accurately tracked and escalated and that Day1 has a comprehensive view of all outstanding action items. Day1 has the processes and procedures in-place to facilitate rapid and quality responses that include centralized team planning and a decentralized execution process. The benefit of this approach to the overall contract is that centralized TO coordination facilitates overall resource tracking leading to the best utilization of resources; better prioritization of tasks; ensures clear communication; enables us to implement a centralized repository for lessons learned; and provide a single focal point. Decentralized TO execution ensures dedication to the task, rapid decision-making capability, and maximum responsiveness for multiple tasks. Our organizational structure, is scalable and enables the Day1 Team to support contract management as well as provide support for any size TO project.

Our Contract Manager and PMs have reach-back to additional Day1 Team members and corporate SMEs. This element of our organizational structure ensures that high quality support is consistently available and delivered to the TOs when needed. In addition, our reach-back capability enables us to respond quickly to new resource requirements and/or surges in workload requirements. As a services organization with Subject Matter Experts, each function within this element is matrixed to the NASPO contract and used as required to satisfy the requirements of individual Purchasing Entities.

Our Contract Manager, PMs, and delivery team will leverage a suite of tools such as MavenLink, Microsoft Project Server, and Microsoft SharePoint as part of the Day1 Project Management Information System (PMIS). Day1 has

implemented SharePoint in the Microsoft O365 cloud, which gives our teams the agility to access and fully utilize this PMIS tool from virtually anywhere. Our PM will create SharePoint sites specifically to suit the need of our NASPO delivery team. Additionally, the system allows for centrally stored and managed program artifacts and enables our team to leverage the real time collaboration features of SharePoint. With strong version control capabilities, user access controls, and strong integration with Windows and Active Directory, we will apply the necessary governance and oversight of all NASPO program documents, artifacts, and deliverables. Additionally, our PM's can leverage tools such as Microsoft Project and MavenLink (please refer to *Section 1.3.7 Project Schedule Plans [RFP 8.3.7]* for more details surrounding MavenLink project scheduling capabilities). Through the use of MavenLink, our PM's can share activities with team members, develop project schedules, track resources time, budget, schedule, and even store deliverables for quality control and quality assurance as seen in the figure below.

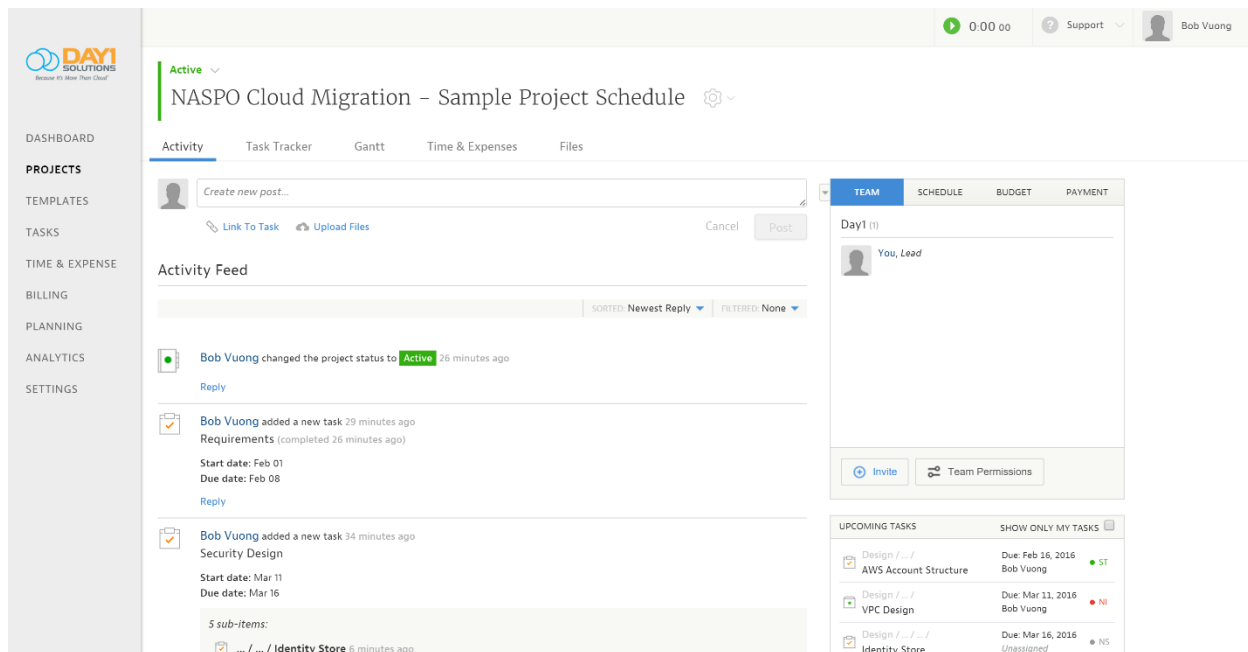


Figure 14: MavenLink as a PMIS tool

Day1 uses a coordinated system of Quality Assurance (QA) and Quality Control (QC) activities that include work product reviews, health checks, program performance surveillance, and quality monitoring to drive continuous improvement. Our Project Management Office (PMO) is managed by our Vice President of Programs and Services, Mr. Bob Vuong. Mr. Vuong will serve as the Reports Administrator for this program and also will be held accountable for developing the quality assurance measures for this vehicle. Mr. Vuong is a Project Management Institute (PMI) certified Project Management Professional (PMP) and has developed the Day1 PMO to institute QC approaches that follow the PMI quality management processes throughout project execution and methodically incorporating QC on all of our IT projects. Our team uses an internally dedicated QC organization with processes that include a structured review and audit of all activities and deliverables to verify they comply with the applicable procedures, standards, and deadlines.

Day1's corporate team works directly with the project delivery team during the early stages of a project to establish plans, standards, metrics, and procedures to ensure that measurable, meaningful, and usable methods are identified for performing reviews and audits throughout the program life cycle. Where necessary we develop a Quality Control

Plan (QCP) that comprehensively defines how Day1 manages the quality of work products for each service contract to meet the program and mission requirements. We accomplish this through the continued application of our Quality Management System that incorporates quality assurance measures throughout project execution as seen in Figure 15 below.



Figure 15: Quality Assurance and Control in Each Day1 Project

- Quality control plans developed during the project planning phase
- QA/QC is part of the continuous delivery cycle throughout execution phase
- QA approaches establish the high-level project planning and management framework that is detailed in execution
- QC Checkpoints review products and services at defined points of production to verify conformance through a rigorous inspection process. For inspections, we utilize statistical sampling to determine the number of pieces to be inspected, which saves time and enhances overall accuracy in the process. We create checklists upstream to ensure technical accuracy.
- QA Checkpoints provide independent examination of process outputs and use subject matter expertise to confirm that final outputs meet the input requirements.

Day1 has compiled an extensive collection of webpages and associated Uniform Resource Locator (URL) specific to AWS services and resources and will make these available to NASPO. The table below is a list of URL's can be accessed directly by NASPO. Additionally, as an AWS Advanced Consulting partner, Day1 has access to the Amazon Partner Network (APN) with a comprehensive library of white papers, operational guides, implementation guides, best practices, etc., (past what is readily accessible to non APN partners) that we will make available to the NASPO as required.

<b>SLA's</b>	EC2 SLA: <a href="http://aws.amazon.com/ec2-sla/">http://aws.amazon.com/ec2-sla/</a>
	S3 SLA: <a href="http://aws.amazon.com/s3-sla">http://aws.amazon.com/s3-sla</a>
	CloudFront SLA: <a href="http://aws.amazon.com/cloudfront/sla/">http://aws.amazon.com/cloudfront/sla/</a>
	Route 53 SLA: <a href="http://aws.amazon.com/route53/sla/">http://aws.amazon.com/route53/sla/</a>
	RDS SLA: <a href="http://aws.amazon.com/rds-sla/">http://aws.amazon.com/rds-sla/</a>
<b>Help Desk and Technical Support</b>	Technical FAQ's - <a href="https://aws.amazon.com/faqs/">https://aws.amazon.com/faqs/</a>
	Support Forums - <a href="https://forums.aws.amazon.com/index.jspa">https://forums.aws.amazon.com/index.jspa</a>
	Support Site - <a href="https://aws.amazon.com/premiumsupport/">https://aws.amazon.com/premiumsupport/</a>
	Trusted Advisors - <a href="https://aws.amazon.com/premiumsupport/trustedadvisor/">https://aws.amazon.com/premiumsupport/trustedadvisor/</a>
<b>Resources</b>	Documentation - <a href="https://aws.amazon.com/documentation/">https://aws.amazon.com/documentation/</a>
	Whitepapers - <a href="http://aws.amazon.com/whitepapers/">http://aws.amazon.com/whitepapers/</a>
	Knowledge Centers - <a href="https://aws.amazon.com/premiumsupport/knowledge-center/">https://aws.amazon.com/premiumsupport/knowledge-center/</a>
	Videos and Webinars - <a href="https://aws.amazon.com/about-aws/events/">https://aws.amazon.com/about-aws/events/</a>

Figure 16: AWS Services and Resources URL's

**Day1's SaaS offering with Infor:** Infor's Incident Management Model includes four main areas:

- Incident/Service Request Entry
- Qualifying
- Research
- Resolution

This model is used for all subscriber incidents and service requests including product issues, product questions, Cloud Environment issues, product update, and cloud service requests.



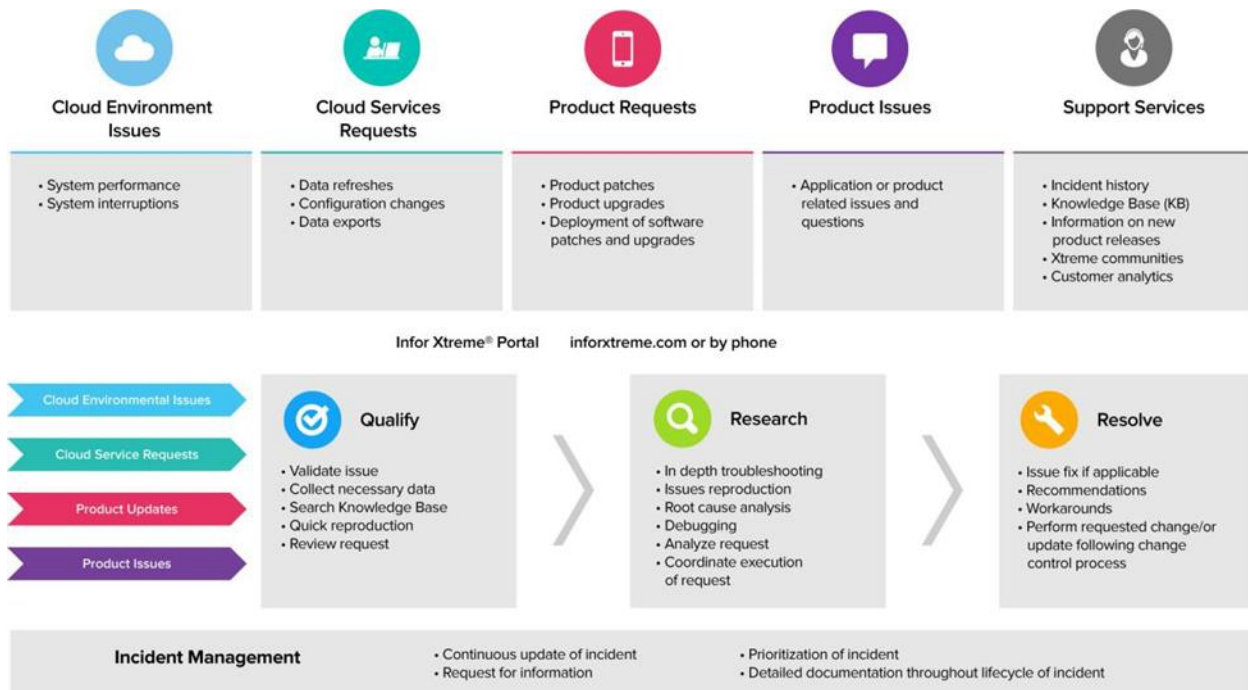


Figure 17: Infor's Incident Management Model

- Incident Entry:** Licensee is able to initiate an incident via the Infor Xtreme® Portal located at [www.infor.com/inforxtreme](http://www.infor.com/inforxtreme) or by calling the Infor Xtreme Support Center. All issues and requests for service or product updates are to be entered into Infor Xtreme®. When a new incident is entered via the Infor Xtreme® Portal, it is automatically routed to the appropriate queue to be picked up by the next available support analyst or, if a cloud environment issue has been reported, Infor's cloud operations resources. Alternately, the Licensee may call Infor Xtreme Support and speak to a member of the Customer Care Team. The Customer Care Team member will ask for specific information, including a short description of the issue. The incident will then be routed to the appropriate queue to be addressed by the next available support analyst or Infor cloud operations resource. Cloud Service requests are also initiated via the Infor Xtreme® Portal. When a Cloud Service request is entered via the Infor Xtreme® Portal, it is automatically routed to the support operations team.

- Qualifying:** Once an incident has been received, the support analyst may contact the Licensee for additional information. Clarification of the incident may be necessary before in-depth analysis can be performed and before the support analyst can begin to resolve the incident. Qualification steps may include, without limitation, searching the Support Knowledge Base, reproducing the reported issue, and/or collecting additional information to validate the issue.

For Cloud Service requests and product updates, a cloud operations staff member will review the request and begin the process of communicating with Licensee to review, scope and begin scheduling

- Research:** Using the results from the Qualifying step, the support analyst will perform further research and testing to help assess the incident. This may include, without limitation, debugging, root cause analysis, reproduction of the issue and in-depth troubleshooting. If the incident requires that a discrepancy record be created, the support analyst will document the steps required and will forward the discrepancy record to the Infor Product Development Team. The analyst will associate the Licensee with the discrepancy, so the Licensee is proactively notified of any updates.

For Cloud Service requests and product updates, Infor’s cloud operations team will analyze the request made by Purchasing Entities, discuss the request with Purchasing Entities, including the scope of effort and whether additional fees will apply, and then establish a plan to execute that request or product update.

- **Resolution:** Once a product issue has been addressed, a service request is executed and/or a product update is installed to resolve the source of an incident, the incident will be closed.

Most product issues are resolved by the support analyst. Where a software fix is required, the Infor Product Development Team is responsible for developing software fixes, as required. Software fixes will be scheduled with priority given to higher severity level issues. The open incident will be updated with the new information. Notwithstanding anything to the contrary set forth above, not all resolutions require a software fix or product modification as some incidents can be resolved with a workaround or other recommendations, as determined in Infor’s sole discretion.

**Incident Management**

- **Incident:** An “incident”, is a single request for assistance or information related to the Subscription Software or Cloud Environment that is fully and accurately logged within the Infor Xtreme® Portal or registered by contacting Xtreme Support via phone. Other commonly used names for an incident are “case,” “inquiry,” “call,” “log,” “issue,” and “ticket.”
- **Severity Levels:** Support incidents are classified according to the following severity level descriptions. Each incident must have a severity level assigned to it and the severity level must be provided as part of the information used to log an incident. Use the following table of definitions as a guide for assigning a severity level.

Severity Level	Description	Examples
1	<b>Production System Down</b>	The environment is not available, or the production system or database is available, but a critical application failure has occurred and business processes are halted. There are no workarounds available.
2	<b>High</b>	A critical business process of the Subscription Software is impaired, causing a serious disruption of a major business function, which is having a serious impact on daily functions or processing, and there is no acceptable workaround.
3	<b>Medium</b>	Non-critical issue has occurred with the Subscription Software. Purchasing Entities are able to run the Subscription Software and there is an acceptable workaround for the issue.
4	<b>Low</b>	An inquiry or low impact issue that does not require immediate attention. This includes cosmetic issues on screens, errors in documentation, or a request regarding use of the Subscription Software

Figure 18: Infor Incident Management

#### 1.4.2 Customer Service Requirements [RFP 8.4.2]

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

- a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.*
- b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.*
- c. Customer Service Representative will respond to inquiries within one business day.*
- d. You must provide design services for the applicable categories.*
- e. You must provide Installation Services for the applicable categories.*

As discussed in *Section 1.4(E) Customer Service [RFP 8.4]* Day1's ValuePoint Contract Administrator, Mr. Sean Wilson, has full authority and autonomy of the contract and will serve as the Day1 lead representative for all entities that execute a Participating Addendum. His information will be kept current and will be accessible through multiple means to include:

- Direct contact of in-person, through email, or phone as provided in our Organizational Profile
- Online self-service for issues that need attention through our NASPO landing page at [www.day1solutions.com/NASPO](http://www.day1solutions.com/NASPO)
- Email group for bulk requests at [NASPO@Day1Solutions.com](mailto:NASPO@Day1Solutions.com)

Additionally, Day1's managed services team provides 24x7 customer support and on-call support desk for relevant services that require immediate resolution. This team uses products such as FreshDesk for ticketing and engineering resource management. Escalation policies and SLAs are used to intelligently distribute tickets to appropriate engineering resources. FreshDesk also serves as a customer portal for 24x7 customer service request, for case management as described in *Section 1.3.1 Working with Purchasing Entities through Data Breaches [RFP 8.3.1]*. Please see *Section 1.19 (E) Integration and Customization [RFP 8.19]* for additional information on our design and installation services.

**Day1's SaaS offering with Infor:** Escalation outside of standard Support procedures is reserved for issues that merit a higher degree of attention, and such escalation is not intended for issues that are well suited to Infor standard Support procedures. If an issue needs a higher level of attention, please contact the regional Xtreme Support Center and request the involvement of an Infor Support Manager. The Customer Care team will escalate the issue and notify the appropriate Support Manager. The Support Manager will promptly assess the situation, contact Licensee to discuss a resolution plan, identify required resources, and implement the resolution plan.

#### **Xtreme Support Coverage Limits:**

Customizations and training are outside of standard Support services and may be provided by Infor Consulting Services (<http://www.infor.com/services/>) or by Infor Campus (<http://www.infor.com/services/education/>).

## Infor Cloud Subscription Xtreme Support Plan

	Description
<b>Telephone Access</b>	Infor's Xtreme Support business hours are generally Monday through Friday, 8:00 am to 5:00 pm, local time, in the time zone designated by Licensee as the primary time zone, excluding holidays observed by Infor, which fall within the applicable coverage window. These hours may vary by Subscription Software product. Please refer to the Infor Xtreme® Portal, as Support hours by Subscription Software are noted in specific Knowledge Base articles.
<b>How to Assistance</b>	Infor will help answer procedural questions, including questions about processes, Subscription Software functionality, and features of generally available Subscription Software.
<b>Defined Incident Response Targets</b>	The Infor Xtreme Support team strives to respond promptly to all requests. The "Response Target(s)" below are calculated as the difference between the time an incident is properly logged into the Infor Xtreme® Portal and the time of Infor's first value-added communication. Value-added communication may include, without limitation, requests for additional information, the collection of error logs, findings from initial issue triage, timeline for the next step, or providing existing information from the Knowledge Base. Infor Xtreme Support will make commercially reasonable efforts to meet the Response Targets set forth below.
<b>Priority Incident Queuing</b>	Incidents are managed based on severity; the most critical issues are handled as a priority.
<b>Severity 1 System Availability</b>	If the Cloud Environment is not accessible, then Purchasing Entities are entitled to access Infor Xtreme Support 24x7x365. Infor will make commercially reasonable efforts to respond within one (1) hour. <b>Note:</b> Severity 1 incidents that occur after standard business hours should be reported by telephone to the local Infor Xtreme Support Center
<b>Severity 1 Application Support 24X5 Critical Incident Support</b>	<p>The Cloud Environment is available, but a critical application failure has occurred and business processes are halted.</p> <p>There are no workarounds available. Infor will make commercially reasonable efforts to respond within one (1) business hour during scheduled business hours.</p> <p>This service will also be available during holidays observed by Infor, which fall within the applicable coverage window. 24x5 coverage begins at 12:00 AM Monday through 11:59 PM Friday local time in Licensee's time zone. Please refer to the Infor Xtreme® Portal at <a href="http://www.infor.com/Inforxtreme">www.infor.com/Inforxtreme</a>, as support hours by Subscription Software product are noted in specific Knowledge Base articles. Note: Severity 1 incidents that occur after standard business hours should be reported by telephone to the local Infor Xtreme Support Center</p>
<b>All other Severity Levels</b>	Infor will make commercially reasonable efforts to respond within two (2) business hours.

Description	
<b>Designated Contacts</b>	Designated Contacts will act as liaisons with the Xtreme Support staff. A licensee is entitled to five (5) Designated Contacts. A Designated Contact must have a thorough understanding of the specific Subscription Software, along with the technical knowledge needed to assist in resolution of the incident. If the Designated Contact lacks the knowledge to assist with the incident, Infor may request that Licensee designate an appropriate representative to assist with management of the incident. If the Designated Contact is not available, this will impact the ability of Infor Xtreme Support analysts to troubleshoot the incident. Designated Contacts must be registered as such in the Infor Xtreme® portal.
<b>Unlimited Incidents</b>	There is no limit to the number of incidents that can be submitted by Designated Customer Contacts.
<b>Upgrades</b>	Infor manages upgrading environments to the current version of the Subscription Software. Licensees will be given notice of an upcoming upgrade, so they can prepare by scheduling training on new features, understand changes as documented in the release notes, etc.
<b>Electronic Support</b>	Infor provides 24x7x365 online access to the Infor Xtreme® Portal.
<b>Support Knowledge Base</b>	Access via the Infor Xtreme® Portal to the Support Knowledge Base and other resources that can help Purchasing Entities quickly find answers to outstanding questions or to learn more about the Subscription Software Purchasing Entities are using.
<b>Subscription Software Information</b>	Access the Infor Xtreme® Portal to obtain information on Subscription Software enhancements, documentation updates, and related release notes.
<b>Critical Solution Notification</b>	The Infor Xtreme® Portal enables each Designated Contact to develop a unique profile. Each Designated Contact may also choose to sign up for Knowledge Base articles of particular interest. When Infor develops a Knowledge Base article for a critical incident, the Designated Contact can receive a notification about its availability.
<b>Recorded Briefings</b>	Infor provides access to recorded webinar briefings, typically 5-15 minutes in length, that are designed to help Licensees become familiar with the latest Subscription Software functions and features.
<b>Infor Xtreme Communities</b>	Communities were developed as a social networking forum to allowing Licensees, Infor partners, and Infor employees to share best practices and possible resolutions to challenging or complex business issues.

Figure 19: Infor Cloud Subscription Xtreme Support Plan

### Infor Cloud Subscription Premium Support Plan

Xtreme Premium Support Plan\*\* Includes all of the features of the Xtreme Support plan plus the following:

Description	
<b>24X7 Critical Incident Application Support</b>	Critical Incident Support for Severity 1 application incidents 365 days a year and 24 hours per day. This service will also be available during holidays observed by Infor.
<b>Live, Interactive Briefings</b>	Attend live briefing sessions throughout the year and ask the analysts questions on general interest topics and recommend topics for future briefings.
<b>Priority Plan Queuing</b>	Incidents are prioritized based upon severity level as well as the applicable Xtreme Support plan. All other factors being equal, Premium and Elite Support plans will generally have a higher priority.

Figure 20: Infor Cloud Subscription Premium Support Plan

### Infor Cloud Subscription Elite Support Plan

Xtreme Elite Support\*\* Includes all of the features of the Xtreme Premium Support plan plus:

Description	
<b>Special Events Support</b>	Get Xtreme Support for all severity levels for one weekend a year. This can be an advantage when planning application upgrades or other company/IT events.
<b>Assigned Customer Success Manager</b>	A designated resource who helps resolve issues through coordination of the following activities: access to senior level Xtreme Support and development analysts; update planning assistance; scorecard reports and early adopter program
<b>Access to senior level Xtreme Support and Development analysts</b>	Where appropriate, the Customer Success Manager will coordinate meetings with senior Support and Development resources to help resolve urgent issues.
<b>Update planning assistance</b>	Work with Infor Xtreme Support to help plan service pack and update installations. The Customer Success Manager will discuss plans, any known issues, and other Support considerations.
<b>Enhanced Response Targets Severity 1 (Production System Down)</b>	Infor will make commercially reasonable efforts to respond to Severity 1 incidents within 30 minutes during scheduled business hours.  <b>Note:</b> All Severity 1 issues which occur outside of standard Xtreme Support hours must be reported by telephone to the local Infor Xtreme Support Center.
<b>All other Severities (except 5)</b>	Infor will make commercially reasonable efforts to respond within one (1) business hour during scheduled coverage hours.
<b>Scorecard Activity Reports</b>	Get regular reports detailing Xtreme Support activity. The Customer Success Manager will analyze the report and make recommendations.
<b>Early Adopter Program</b>	Obtain insight into planned products and Component System enhancements, as well as the opportunity to participate in beta or early adopter programs.

Description	
<b>Infor Education Incentives</b>	Eligibility for discounts on Infor Campus Card.

Figure 21: Infor Cloud Subscription Elite Support Plan

## 1.5 (E) Security of Information [RFP 8.5]

### 1.5.1 Data Protection [RFP 8.5.1]

*Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.*

As an AWS authorized partner, Day1 will leverage the AWS Federal Risk and Authorization Management Program (FedRAMP) certifications in the development of cloud based solutions for NASPO and their customers. AWS is a FedRAMP Compliant Cloud Service Provider (CSP). AWS has completed the testing performed by a FedRAMP-accredited Third Party Assessment Organization (3PAO) and has been granted two Agency Authority to Operate (ATOs) by the US Department of Health and Human Services (HHS). AWS' compliance with FedRAMP requirements was achieved based on testing performed against the stringent NIST 800-53 Rev. 3 – Moderate baseline requirements, plus additional FedRAMP security controls. The HHS authorization is at the Moderate impact level to store, process, and protect a diverse array of sensitive government data.

Day1 believes that NASPO requires a cloud vendor to have fully developed AWS capabilities to ensure that NASPO purchasing entities have a clear understanding of to how they store, manage, and protect their data. There are four important basics regarding data ownership and management in the shared responsibility model:

1. Customers continue to own their data.
2. Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
3. Customers can download or delete their data whenever they like.
4. 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's operating model clearly delineates the responsibility of controls between AWS and its customers. AWS's shared responsibility/security model is outlined below.

- **AWS Responsibility** - AWS operates, manages and controls the infrastructure components, from the host operating system and virtualization layer, down to the physical security of the facilities in which the service operates.
- **Customer/Partner Responsibility** – Customers/Partners assume responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS provided security group firewalls and other security, change management and logging features.

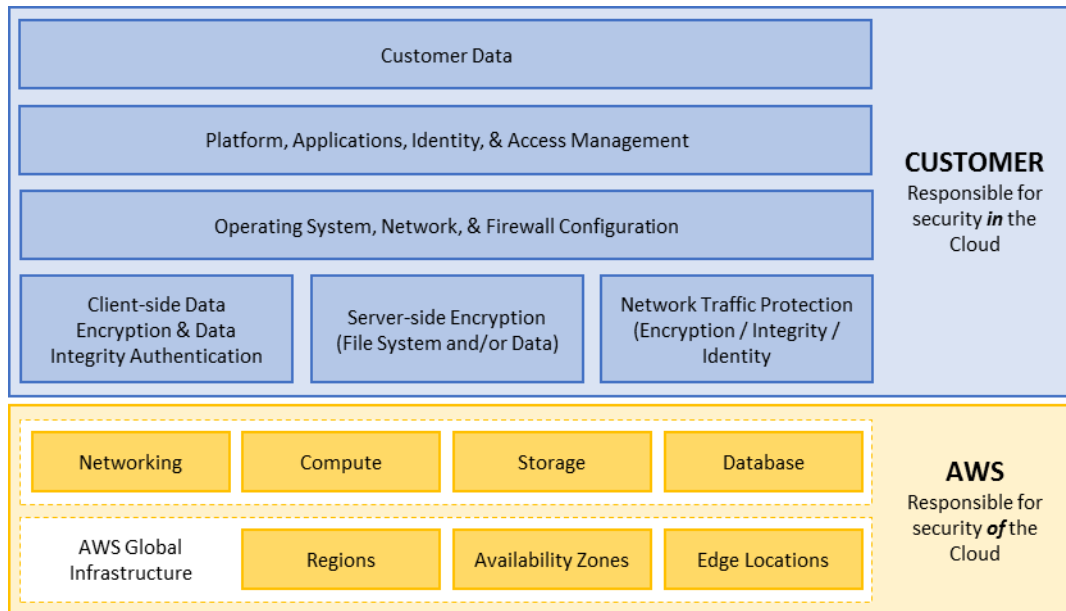


Figure 22: AWS Shared Responsibility Model

In support of the shared responsibility model (Figure 22: AWS Shared Responsibility Model), Day1 will help to implement a wide variety of security services for NASPO’s cloud based environment to provide greater control over services categorized as “Customer” responsibility in the shared model. These services include network security, access control, monitoring & logging, backup & replication, and data encryption. A brief synopsis of these services that support the security of information include the following:

<b>Network Security</b>	Developing virtual and/or logical private cloud segments helps to increase network security and allows for NASPO to control cloud resource communications. Day1 can assist in developing the network architecture and defining security inspection, detection, and monitoring points.
<b>Access Control</b>	Multiple layers of access control allow only NASPO’s authorized users, customers, and applications to access cloud based resources. Options such as setting up access control policies, individual user accounts, and unique credentials help to secure these controls.
<b>Monitoring &amp; Logging</b>	Cloud based resources require a much more integrated monitoring tool for keeping track of and monitoring cloud resources. The monitoring and logging capabilities Day1 can help to implement can provide instant visibility into NASPO’s inventory as well as user and application activity.
<b>Backup &amp; Replication</b>	NASPO’s security strategy should include regular backups or snapshots of cloud based objects and data. In many cases, backups can be setup to occur automatically, and in other cases, NASPO can configure snapshots using a variety of backup options.
<b>Data Encryption</b>	Day1 believes in using encryption wherever possible, and enabling NASPO with multiple encryption methodologies. For instance, encrypting data at rest or in transit may be a requirement or security regulation that NASPO will look to follow.



#### Data Archival

With Amazon S3's lifecycle policies, NASPO customers can configure their data stores to be archived to Amazon Glacier or deleted after a specific period of time. Day1 can support NASPO in using policy-driven automation to quickly and easily reduce storage costs, as well as, save time. With this, NASPO customers can specify a prefix, a time period, a transition to Amazon Glacier, and/or an expiration. Lifecycle policies apply to both existing and new S3 objects, ensuring that NASPO 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.

*Figure 23: Security Services*

**Day1's SaaS offering with Infor:** Infor's Architects have designed a unique environment within Amazon Web Services (AWS), which provides failover redundancy. AWS provides multiple data centers across various geographic regions and multiple Availability Zones (AZ) within those regions which support high-availability, fault tolerance, and seamless failover capabilities. We perform frequent full database backups, differential backups, and transaction log backups. The backups are copied across all three nodes and snapshots are taken to ensure recoverability throughout our retention period. Database restore testing is conducted every 90 days on all clusters in order to verify that backups are good.

The Infor SaaS multi-tenant cloud environment aligns to CIS standards and best practices. We leverage CIS benchmarks to build standard hardened systems; gold images are configured with anti-virus and anti-malware APIs.

Infor works with AWS to secure all information on multiple levels. All information passes through utilizing TLS/SSL technology and at rest utilizing Transparent Data Encryption (TDE) with AES-256.

Additionally, Infor follows ITIL 2.0 standards. Following these standards allow us and our customers to see the exact access and process that is followed while Infor is working with the applications or the supporting infrastructure.

Finally, physical security is AWS's responsibility as they manage their own data centers. Storage devices that are no longer used are degaussed or destroyed in compliance with procedures described in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization").

#### 1.5.2 Comply with Applicable Laws [RFP 8.5.2]

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

While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would in an on-site datacenter. Day1's works with Participating State's CIOs and other representatives to identify any applicable laws related to data privacy and security. Our cloud architects and SMEs provide. We ensure compliance with applicable with annual security compliance and privacy training as well as situational awareness training.

### 1.5.3 Accessing Purchasing Entity's user accounts or data [RFP 8.5.3]

*Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.*

Day1 can help to educate and inform NASPO Purchasing Entities on the AWS Shared Responsibilities model as described in *Figure 22: AWS Shared Responsibility Model in Section 1.5.1 Data Protection [RFP 8.5.1]*. Through this shared responsibilities model, Day1 believes that NASPO customers will gain assurance that purchasing entity's user accounts, and data remain inaccessible to Day1 or AWS staff except for in the course of daily operations, response to services and expressed terms of the Master Agreement. There are four important basics regarding data ownership and management in the shared responsibility model:

1. Customers continue to own their data.
2. Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
3. Customers can download or delete their data whenever they like.
4. 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.

## 1.6 (E) Privacy and Security [RFP 8.6]

### 1.6.1 Commitment to Industry Standards [RFP 8.6.1]

*Offer must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in **Attachment D**, including supporting the different types of data that you may receive.*

As stated in *Section 1.1.2 NIST Characteristics [RFP 8.1.2]* Day1 understands the importance of complying with NIST characteristics. Day1 is committed to providing solutions that comply with NIST regulations and the requirements of Attachments C & D. Please refer to *Section 1.1.2 NIST Characteristics [RFP 8.1.2]* for more information.

### 1.6.2 Organization Security Certifications [RFP 8.6.2]

*Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.*

As an AWS partner we offer our clients/customers access to a significant list of AWS best practices, security frameworks, certifications, and compliance standards. The list below provides customers with the security standards, which work with the AWS Shared Security model that outlines the responsibilities for security and compliance in a customer environment. The AWS cloud infrastructure has been designed and is managed in alignment with regulations, standards, and best practices. The following list includes security, and industry certifications attained by AWS:

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

Figure 24: AWS Security and Industry Certifications

**Day1's SaaS offering with Infor:** Infor's cloud environment undergoes independent assessments annually, which include, but are not limited to: SSAE 16 SOC 1 Type II, HIPAA, NIST 800-53, etc.

### 1.6.3 Security Practices [RFP 8.6.3]

*Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.*

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. 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.

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.

By default, the AWS network provides significant protection against traditional network security issues, and Day1 can implement further protection to ensure a greater security in depth. The following are a few examples:

<b>Distributed Denial of Service (DDoS) Attacks</b>	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.
<b>Man in the Middle (MITM) Attacks</b>	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.
<b>IP Spoofing</b>	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.
<b>Port Scanning</b>	Unauthorized port scans by Amazon EC2 customers are in direct 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: <a href="http://aws.amazon.com/contact-us/report-abuse/">http://aws.amazon.com/contact-us/report-abuse/</a> . 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.
<b>Packet sniffing by other tenants</b>	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 interfaces can be placed into promiscuous mode, the hypervisor will not deliver any traffic 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 Address Resolution Protocol (ARP) cache poisoning do not work within Amazon EC2 and Amazon Virtual Private Cloud (VPC). While Amazon EC2 does provide ample protection against one customer inadvertently or maliciously attempting to view another’s data, as a standard practice all sensitive traffic should be encrypted.

Figure 25: AWS Security Services

Day1 has access to several security information and event management (SIEM) providers and has the in house ability to implement these toolsets in order to develop a holistic view of the security posture of the NASPO network and IT infrastructure. We can develop a SIEM strategy that focuses on capturing and analyzing logs from multiple sources such as user activities, application usage patterns, system logs, and other security related events. Our experiences with SEIM in cloud environments is that they often have several gaps and weaknesses and typically not replicate the

capabilities of an enterprise architecture. An integration of native and third party products are often used in filling those gaps. Day1 may leverage tools like Splunk as a SIEM tool for IaaS and PaaS implementations. Splunk Enterprise is a massively scalable data engine for machine-generated data. It collects, indexes, and harnesses machine data across an infrastructure in real time. Splunk offers a cost effective and flexible way to meet compliance requirements from audit trail collection and reporting, to file integrity monitoring with a single solution. The additional benefits of using Splunk include:

- E-Discovery - Search every data source required for E-Discovery from one place. Get instantaneous results across large data sets.
- FISMA - Securely collect, index and store all log and Machine Data along with audit trails to meet NIST requirements.
- HIPAA - Search all machine data to instantly assess reports of EPHI leakage and meet HIPAA's explicit log requirements.
- PCI - Rapid compliance with explicit PCI requirements for log retention/review and change monitoring, comprehensive reporting on all PCI controls such as passwords and firewall policy.
- SOX - Splunk makes the ambiguous chore of compliance-mandated routine log review easy and straightforward.

**Day1's SaaS offering with Infor:** Infor has implemented encryption of data at rest and in-transit. Additionally, customers are provisioned with a unique tenant ID, which is also used to provision their unique logical database.

Infor leverages the physical security of AWS's state-of-the-art data centers, which are housed in nondescript facilities, and to which physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. All physical access to data centers by AWS employees is logged and audited routinely.

#### 1.6.4 Data Confidentiality Standards [RFP 8.6.4]

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

Day1's AWS solution does not require access to customer data, and customers are given the choice as to how they store, manage and protect their data. Please refer to *Section 1.5.1 Data Protection [RFP 8.5.1]* and *Section 1.5.3 Accessing Purchasing Entity's user accounts or data [RFP 8.5.3]* for more information.

**Day1's SaaS offering with Infor:** Infor has implemented role-based access controls (RBAC), so that Infor staff is only granted access to the Cloud environment based on the need to perform their respective job responsibilities. Access is regularly monitored and reviewed. Additionally, the Infor Cloud Security Policy includes guidelines that provide acceptable use policies for the use of hardware and software.

### 1.6.5 Third-Party attestations, Reports, Security Credentials, and Certifications [RFP 8.6.5]

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

Please refer to *Section 1.6.2 Organization Security Certifications [RFP 8.6.2]* for more information pertaining to the list of third-party attestations, reports, security credentials, and other controls obtained by AWS.

**Day1's SaaS offering with Infor:** Infor is currently pursuing FedRAMP authorization, which is based on NIST 800-53 information security controls. Infor has contracted with a third-party contractor, Kratos SecureInfo to facilitate our authorization process.

### 1.6.6 Logging Process [RFP 8.6.6]

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

Day1 can support NASPO's need for a robust logging process using multiple AWS features and capabilities such as AWS CloudTrail, CloudWatch, and LogAnalyzer (along with third-party tool) to monitor instances, manage, and analyze log files. AWS CloudTrail is a web service that can be setup to record specific Application Program Interface (API) calls to supported AWS services in. These records can be delivered into a log file to an Amazon Simple Storage Service (Amazon S3) bucket. AWS CloudTrail can alleviate common challenges experienced in an on-premise environment by NASPO customers, making it easier for these organizations to enhance security and operational processes while demonstrating compliance with policies or regulatory standards. With AWS CloudTrail, NASPO 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.

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. Day1 can guide NASPO customers to use CloudWatch Logs to monitor and troubleshoot systems and applications using existing system, application, and custom log files. Our team can help setup a strategy for shipping existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time. This helps NASPO customers better understand and operate their systems and applications, and they can store their logs using highly durable, low-cost storage for later access.

Day1 can also help to implement LogAnalyzer for Amazon CloudFront for NASPO customers who want to analyze their Amazon CloudFront Logs using Amazon Elastic MapReduce (Amazon EMR). Using Amazon EMR and the LogAnalyzer application NASPO customers can generate usage reports containing total traffic volume, object popularity, a breakdown of traffic by client IPs, and edge location. LogAnalyzer application produces four sets of reports based on Amazon CloudFront access logs. Reports are formatted as tab delimited text files, and delivered to the Amazon S3 bucket that customers specify.

- 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.

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.

**Day1's SaaS offering with Infor:** Infor leverages a security information and event management (SIEM) solution, which captures logs from systems and stores them in an immutable location. The events which are captured include, but are not limited to: failed login attempts, successful logins, etc.

#### 1.6.7 Visibility Restriction [RFP 8.6.7]

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

Day1 can restrict visibility of NASPO customer cloud hosted data to specific users and groups through role based access control using the AWS Identity and Access Management (IAM) tool. AWS IAM allows NASPO purchasing entities to control the level of access they have to AWS resources. AWS IAM is a web service that enables AWS customers to manage users and user permissions in AWS. 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. 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 this tool, NASPO customers can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access. Day1 can guide NASPO entities in setting proper permissions to specify who has access to AWS resources and which actions they can perform on those resources.

**Day1's SaaS offering with Infor:** Infor restricts visibility of cloud hosted data and documents to specific users or groups by leveraging AWS's network access controls (ACLs), Identity and Access Management (IAM) roles, and security groups.

#### 1.6.8 Security Incident Notification Process [RFP 8.6.8]

*Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.*

Day1 leverages multiple mechanisms to allow our customer support team to be notified of operational issues that impact the customer experience. An AWS "Service Health Dashboard" is available and maintained by AWS customer support team to alert customers to any issues that may be of broad impact. The "AWS Security Center" can be leveraged by NASPO purchasing entities for security and compliance details about AWS. NASPO customers can also subscribe to AWS Support offerings that include direct communication with the customer support team and proactive alerts to any customer impacting issues.

**Day1's SaaS offering with Infor:** Infor's Security Incident procedure follows a similar process as other Cloud Support incidents. After an incident as occurred, Infor's Security Officer or designee notifies affected customers, insurance carriers, third party providers and/or law enforcement as necessary. Cybersecurity incident notifications are handled in a more discreet manner than other incidents, usually via phone call or confidential email.

Infor notifies affected customers of a confirmed breach involving their data as quickly as reasonably possible, typically within 48 hours of confirmation of such an incident.

### 1.6.9 Security Controls [RFP 8.6.9]

*Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.*

Day1 proposes the implementation of Amazon Virtual Private Cloud (VPC) to provide security controls and boundaries and to isolate hosted servers. The design, engineering, and implementation of Amazon VPC provides the NASPO customers with isolated hosted server deployments. Amazon VPC includes the following characteristics:

- Provision logically isolated computing/processing resources to host NASPO customer applications/systems.
- Isolated network that can be user defined to host the required NASPO customer applications/systems.
- Controlled access to VPC can be established through VPN connections.
- Additional tools and services can be configured to provide encryption in-transit and at-rest capabilities.
- Dedicated instances provides greater isolation and private cloud-like performance with computing instances on single-tenant compute hardware. This will ensure that sensitive data and compute has dedicated processing that only serve designated NASPO customer resources.

Using VPC's NASPO customers can have complete control over virtual networking environment, including selection of IP address ranges, creation of subnets, and configuration of route tables and network gateways. NASPO customers can easily customize the network configuration for their VPC such as creating a public-facing subnet for web servers that have access to the Internet, and placing backend systems such as databases or application servers in a private-facing subnet with no Internet access. Day1 can also help to leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

**Day1's SaaS offering with Infor:** Infor has partnered with Amazon Web Services (AWS). Our Cloud Architecture leverages AWS private subnets, referred to as Virtual Private Clouds (VPCs). VPCs are deployed in AWS Availability Zones (AZs), which are separate data centers within dispersed geographic regions. Testing and staging environments are segmented from production in a separate VPC subnet.

### 1.6.10 Security Technical Reference Architecture [RFP 8.6.10]

*Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).*

Day1 will support the implementation of cloud based solutions in AWS through a Security Technical Reference Architecture known as the AWS GoldBase. AWS GoldBase is a reference architecture that enables customers to streamline, automate, and implement secure baselines in AWS, from initial design to operational secure readiness. AWS GoldBase incorporates the expertise of AWS solutions architects, as well as security and compliance personnel,



to build a secure and reliable architecture in an easy-to-implement package through automation. The AWS GoldBase solution includes the following items for customer use:

- **Security Control Responsibility Matrix (CRM)** - The AWS GoldBase solution includes a security CRM, which maps features and resources to specific security controls requirements. Security, compliance and audit personnel can leverage these documents as a reference for making certification and accrediting of systems in AWS easier. The matrix outlines control implementation reference architecture and evidence examples, which meets the security control “risk mitigation” for the AWS customer environment.
- **Architecture Diagrams** - Architectural diagrams are included with the AWS GoldBase solution. These diagrams illustrate and document the design. They provide a visual reference that demonstrates the components deployed by the AWS CloudFormation templates. These diagrams accompany the description of security features implemented by the AWS GoldBase templates.
- **AWS CloudFormation templates** - The AWS GoldBase offering includes AWS CloudFormation templates, which enable recommended automated deployments of a secure and compliant baseline architectures. The default AWS GoldBase solution consists of four JSON (JavaScript Object Notation) template files, which can be launched as stacks using the AWS CloudFormation service.
- **User Guides and deployment instructions** - The AWS GoldBase solution includes a user guides, which provide step-by-step instructions on how to deploy services using the AWS CloudFormation templates, as well as instructions for creating AWS Service Catalogs products and portfolios and for enabling versioning to support automatic distribution to all users who have access to the product and portfolios. Additionally, AWS Service Catalog customers can apply AWS Identity and Access Management (IAM) permissions to control who can view and modify products and portfolios as well as apply constraints to restrict specific AWS resources.

#### 1.6.11 Security Procedures [RFP 8.6.11]

---

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

As discussed in *Section 1.5.1 Data Protection [RFP 8.5.1]* AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and customers are responsible for securing the workloads they deploy in AWS. AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts pre-employment criminal background checks, as permitted by law, for employees commensurate with their position and level of access. The AWS SOC reports provides additional details regarding the controls in place for background verification.

#### 1.6.12 Security Measures and Standards [RFP 8.6.12]

---

*Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.*

Please refer to *Section 1.9.1 Encryption Technologies [RFP 8.9.1]* for more information on securing data at rest and in transit.

### 1.6.13 Notification Policies and Procedures [RFP 8.6.13]

---

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

As discussed in *Section 1.5.1 Data Protection [RFP 8.5.1]* AWS operates under a shared security responsibility model, and AWS Customers retain the responsibility to monitor their own environment for privacy breaches. Day1 can assist in this monitoring through our managed services team.

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

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

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

## 1.7 (E) Migration and Redeployment Plan [RFP 8.7]

---

### 1.7.1 End of Life Activities [RFP 8.7.1]

---

*Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.*

AWS 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/>.

**Day1's SaaS offering with Infor:** Infor follows NIST 800-88 / DoD 5220-22m to securely scrub data and decommission hardware that was once in use.

### 1.7.2 Return of Data [RFP 8.7.2]

*Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.*

AWS does not access customer data, and customers are given the choice as to how they store, manage and protect their data. Please refer to *Section 1.5.1 Data Protection [RFP 8.4.1]* and *Section 1.5.3 Accessing Purchasing Entity's user accounts or data [RFP 8.5.3]* for more information.

**Day1's SaaS offering with Infor:** Infor helps our customers move their data back on premise or to another Cloud provider. We recommend the use of an sFTP for the transfer of the data.

## 1.8 (E) Service or Data Recovery [RFP 8.8]

### 1.8.1 Situational Response [RFP 8.8.1]

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

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

Day1's managed services team will work with NASPO customers to define a schedule for routine downtime for maintenance. In the event of extended downtime for any reason, Day1 will utilize existing escalation and notification policies to communicate timelines with NASPO customers and minimize the extended downtime. Should an unrecoverable loss of data occur, Day1 will leverage snapshots and automated restore processes to return the affected instances and services to a working state. If upon investigation of the data loss Day1 MSP is at fault for failing to meet an SLA or has failed to follow determined Backup/DR policy, service credit will be awarded based on severity of data loss and agreement between Day1 and NASPO customer.

There are several options for contingency and response to business failure, one option is to have a pilot light infrastructure built and ready to continue business operations in the event of a failure. A pilot light is a small part of the infrastructure always running, synchronizing mutable data (as Databases or documents) and a mirror group of servers configured to, when turned on to replace the original structure rapidly and with little administrative effort. Day1 will guide NASPO customers to understand the required cost and benefit of a tailored DR plan that meets the requirements of the specific environment.

Our backup methodologies and the inherent flexibility of the AWS software-defined infrastructure enable Day1 to automate the heavy lifting of the disaster recovery process. Amazon Machine Images (AMIs) are leveraged in conjunction with incremental snapshots to minimize the amount of time it takes to restore the affected services in the event of a severe system outage. At the moment an event has been detected monitoring toolsets would report

the event to the responsible Day1 MSP Engineer, this is achieved through auto-escalated ticketing policies and a virtual paging system. The engineer would then notify the affected customer of the incident and start determining overall impact. They would then restore affected instances from most recent snapshot. Once recovery is complete Day1 MSP engineer would communicate with NASPO customer POC and assist in validating the recovered instances, restoring application data as required, determining the extent of impact, as well as investigating cause of the system outage. Day1 will establish acceptable Recovery Point Objective (RPO) and Recovery Time Objective (RTO) with NASPO customers per environment. Day1's RPO and RTO depend heavily on the requirements of the environment. AWS is inherently agile and can be structured to support even the most demanding requirements for DR. Day1 would advise NASPO customers to choose the RPO/RTO metrics that best meet their needs while managing cost and expectation.

**Day1's SaaS offering with Infor:** Infor has partnered with AWS as our infrastructure and DR partner. This infrastructure is designed with geographically dispersed Regions, Availability Zones (AZ)/Data centers and Virtual Private Clouds (VPC). All Production and Test environment data is backed up in all AZ's within an individual Region and can be architected to be backed up in multiple regions.

### 1.8.2 Backup and Restore Methodology [RFP 8.8.2]

*Describe your methodologies for the following backup and restore services:*

- a. Method of data backups*
- b. Method of server image backups*
- c. Digital location of backup storage (secondary storage, tape, etc.)*
- d. Alternate data center strategies for primary data centers within the continental*

As NASPO customers begin to adopt the AWS platform, Day1 will guide them through different methods for backup and restore methodologies such as methods for data backups and server image backups. 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.

Day1 asserts that these characteristics offer NASPO customers opportunities to recover deleted or corrupted data with less infrastructure overhead and puts emphasis on protecting configurations rather than actual servers. 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. *Figure 26: Amazon EC2 Backup Approach* below depicts an Amazon EC2 backup approach and a sample workflow of a server image creation 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.

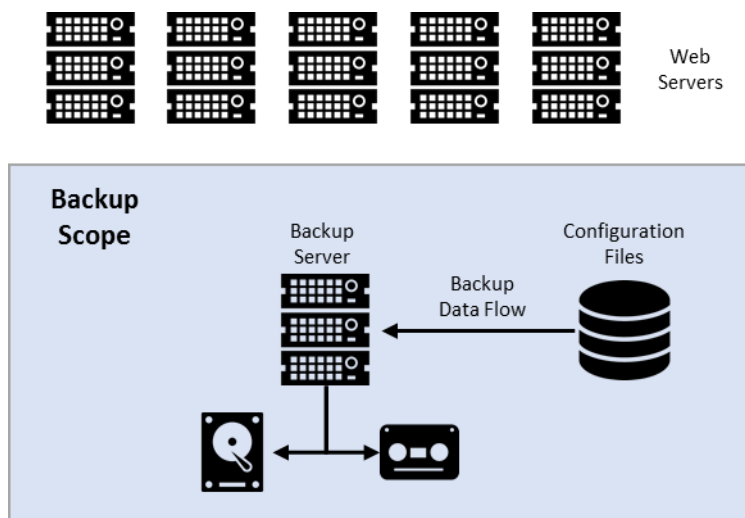


Figure 26: Amazon EC2 Backup Approach

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).

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, NASPO customers can create totally independent copies of AMIs 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.

As described above, another factor of a successful backup and recovery method includes the management of configuration files. Day1 can help manage configuration files leveraging NASPO customer's existing version

management software. NASPO customer's may use a variety of version management approaches for configuration files, and can follow the same regime for the files used to configure their Amazon EC2 instances. For example, a different versions of configuration files can be stored in designated locations and securely controlled like any other code. That code repository can then be backed up using the appropriate backup cycle (e.g., daily, weekly, monthly) and snapshots to protected locations. Furthermore, Day1 can also provide the ability to use Amazon S3 to store 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.

Day1 understands that backing up data for database and file servers is different from web and application servers as they generally contain larger amounts of business data that must be retained and protected at all times. In these cases, Day1 suggest the use of 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. Please refer to *Section 1.15.1 Methodologies for Backup and Restore Services [RFP 8.15.1]* for additional information on Methodologies for Backup and Restore Services.

**Day1's SaaS offering with Infor:** Infor's backup and disaster recovery information is provided in 1.15 (E) Backup and Disaster Plan, later in this document. Infor has partnered with AWS as our infrastructure and DR partner. This infrastructure is designed with geographically dispersed Regions, Availability Zones (AZ)/Data centers and Virtual Private Clouds (VPC). All Production and Test environment data is backed up in all AZ's within an individual Region and can be architected to be backed up in multiple regions.

## 1.9 (E) Data Protection [RFP 8.9]

---

### 1.9.1 Encryption Technologies [RFP 8.9.1]

---

*Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.*

AWS customers retain control and ownership of their data, and all data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers should consider the sensitivity of their data and decide if and how they will encrypt data while it is in transit and while it is at rest.

#### 1.9.1.1 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.

### 1.9.1.2 Securing Data in Transit

---

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

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

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

**Day1's SaaS offering with Infor:** Infor utilizes TDE with AES-256 for data at rest and TLS/SSL for data in transit.

### 1.9.2 Business Associate Agreement [RFP 8.9.2]

---

*Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.*

Day1 asserts that it is willing to sign relevant and applicable Business Associate Agreements or any other agreements that may be necessary to protect data with a Purchasing Entity.

### 1.9.3 Data use in alignment with Master Agreement [RFP 8.9.3]

---

*Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.*

AWS does not access customer data, and customers are given the choice as to how they store, manage and protect their data. Please refer to *Section 1.5.1 Data Protection [RFP 8.5.1]* and *1.5.3 Accessing Purchasing Entity's user accounts or data [RFP 8.5.3]* for more information.

Day1's engagement with NASPO purchasing entities will outline access levels and describe account privileges. Day1 uses multiple levels of control including using elevated privileges only when required, using role based authentication, and AWS IAD to control access to data for the intended purpose of each engagement.

## 1.10 (E) Service Level Agreements [RFP 8.10]

---

### 1.10.1 Negotiable SLA [RFP 8.10.1]

---

*Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.*

AWS specific SLAs as described in *Section 1.12.2 Standard Uptime [RFP 8.12.2]* are non-negotiable and are defined as part of each customer agreement. Day1 understands that NASPO may find it desirable to negotiate SLAs; however, Day1 believes that the negotiation of cloud based SLA's may be counter-productive to realizing cost savings through

economies of scale. SLAs for cloud based services are developed based on the cloud provider's ability to meet a specific performance level for each deployment model or service. Negotiating SLAs could force cloud providers to develop agreements, metrics, monitoring services, charge back policies, reimbursement procedures, escalation procedures, etc., that are specific to each individual account. This can negate the economies of scale realized from the masses as everyone shares in the cost associated with managing, maintaining, and operating the environment.

Day1's MSP specific SLA's are non-negotiable; however, are modified based on the support needs acquired by each customer. Day1 provides 3 levels of support and provides SLAs that are specific to those levels of support. Please refer to *Figure 44: High-Level Day1 MSP Offerings* for more information on these SLAs.

### 1.10.2 Sample SLA [RFP 8.10.2]

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

Please refer to *Section 1.12.2 Standard Uptime [RFP 8.12.2]* for additional information on sample SLAs.

**Day1's SaaS offering with Infor:** Infor's standard SLA is 99.5% uptime.

### 1.11 (E) Data Disposal [RFP 8.11]

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

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.

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.

Day1 has identified that Multi-Object Delete can be used by NASPO to delete large numbers of objects from Amazon Simple Storage Service (S3). This feature allows customers to send multiple object keys in a single request to speed up deletion. Amazon does not charge customers for using Multi-Object Delete. Additionally, Day1 can support NASPO in using the Object Expiration feature to remove objects from their Amazon S3 buckets after a specified number of days. With Object Expiration, NASPO can define the expiration rules for a set of objects in S3 buckets through the Lifecycle Configuration policy that can be applied to the S3 bucket.

**Day1's SaaS offering with Infor:** Physical security is AWS's responsibility as they manage their own data centers. Storage devices that are no longer used are degaussed or destroyed in compliance with procedures described in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization").



## 1.12 (E) Performance Measures and Reporting [RFP 8.12]

### 1.12.1 Guarantee Reliability [RFP 8.12.1]

*Describe your ability to guarantee reliability and uptime greater than 99.9%. Additional points will be awarded for 99.99% or greater availability.*

**Day1's SaaS offering with Infor:** Infor's standard SLA is 99.5%. Historically, Infor has provided 99.999% availability for the past 10 years.

Availability for the Subscription Services is measured monthly as a percentage of Scheduled Available Minutes.

- **Scheduled Available Minutes** are the total minutes in a month less the number of Scheduled Maintenance minutes in the applicable month.
- **Available Minutes** is the number of Scheduled Available Minutes in a month less the aggregate number of minutes the Subscription Services were unavailable outside of Scheduled Maintenance.
- **Availability** is a percentage calculated as the Available Minutes in a month divided by the Scheduled Available Minutes in the month.

For example, in a 30 day month with 4 weekly Scheduled Maintenance windows of 8 hours, there are 41,280 Scheduled Available Minutes ((60 min. x 24 hrs. x 30 days)-(60 min. x 8 hrs. x 4 weeks) = 41,280). If the Subscription Services experienced an outage of two hours outside of Schedule Maintenance, there were 41,160 Available Minutes in the month (41,280 Scheduled Available Minutes – 120 minutes of unavailability). The resulting Availability percentage is 41,160 / 41,280 = 99.7%.

### 1.12.2 Standard Uptime [RFP 8.12.2]

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

As described in *Section 1.4.1 Customer Service [RFP 8.4.1]*, Day1 can pass along AWS specific SLA's to NASPO purchasing entities. AWS currently provides SLAs on a service by service basis, and not all services currently have fully defined SLA's. The current list of AWS products with SLAs include EC2, S3, CloudFront, Route53, and RDS. *Figure 27: AWS SLAs and Consequences* below provide a list of AWS services, the outlined monthly uptime, and consequences to AWS if specified criteria are not achieved.

Service	Monthly Uptime Percentage	Service Credit
EC2	Less than 99.95% but equal to or greater than 99.0%	10%
	Less than 99.0%	30%
	Equal to or greater than 99.0% but less than 99.9%	10%
S3	Less than 99.0%	25%
	Equal to or greater than 98.0% but less than 99.0% (for S3 Standard - Infrequent Access)	10%
	Less than 98.0% (for S3 Standard - Infrequent Access)	25%
CloudFront	Equal to or greater than 99% but less than 99.9%	10%
	Less than 99%	25%

Service	Monthly Uptime Percentage	Service Credit
<b>Route53</b>	Route 53 was not 100% Available: 5-30 minutes	1 Day Service Credit
	Route 53 was not 100% Available: 31 minutes - 4 hours	7 Days Service Credit
	Route 53 was not 100% Available: More than 4 hours	30 Days Service Credit
<b>RDS</b>	Less than 99.95% but equal to or greater than 99.0%	10%
	Less than 99.0%	30%

Figure 27: AWS SLAs and Consequences

- **Day1's SaaS offering with Infor:** Please refer to the response above in *Section 1.12.1 Guarantee Reliability [RFP 8.12.1]*.

### 1.12.3 Support Process [RFP 8.12.3]

*Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.*

Day1 will provides all NASPO purchasing entities with the ability to procure and obtain multiple layers and types of support for their specific cloud requirements. As a certified AWS MSP our organization can provide NASPO customers with complete flexibility in managing their AWS environment. Our MSP practice are ideal for Purchasing Entities who want to mitigate the risk and management of the AWS Shared Responsibility Model as seen in *Section 1.5.1 Data Protection [RFP 8.5.1]*. We provide the additional support services past the IaaS support provided by AWS. For more information on our Managed Services please see the following sections and figures:

- *Section 1.21 (E) Related Value-Added Services to Cloud Solutions [8.21]*
- *Figure 44: High-Level Day1 MSP Offerings*
- *Figure 45: Day1 MSP SLAs Overview*
- *Figure 46: Day1 MSP Severity Levels Description*

Additionally, Purchasing Entities will be provided the multiple options for differing levels of AWS support through Day1 to support the most simple levels of their IaaS environment. At the basic level, NASPO purchasing entities will have 24x7 access to AWS customer service, documentation, whitepapers, and support forums. The additional levels of AWS support that may be procured through Day1 include Developer, Business, and Enterprise. A description of each support level can be seen below:

	Basic	Developer	Business	Enterprise
<b>Customer Service and Communities</b>	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums	24x7 access to customer service, documentation, whitepapers, and support forums

	Basic	Developer	Business	Enterprise
<b>Best Practices</b>	Access to 4 core Trusted Advisor checks	Access to 4 core Trusted Advisor checks	Access to full set of Trusted Advisor checks	Access to full set of Trusted Advisor checks
<b>Technical Support</b>		Business hours* access to Cloud Support Associates via email	24x7 access to Cloud Support Engineers via email, chat & phone	24x7 access to Sr. Cloud Support Engineers via email, chat & phone
<b>Who Can Open Cases</b>		One primary contact/ Unlimited cases	Unlimited contacts/ Unlimited cases (IAM supported)	Unlimited contacts/ Unlimited cases (IAM supported)
<b>Case Severity/ Response Times</b>		Normal: < 12 hours Low: < 24 hours	Urgent: < 1 hour High: < 4 hours Normal: < 12 hours Low: < 24 hours	Critical: < 15 minutes Urgent: < 1 hour High: < 4 hours Normal: < 12 hours Low: < 24 hours
<b>Architecture Support</b>		General guidance	Contextual guidance based on use-case	Consultative review and guidance based on applications and solutions
<b>Launch Support</b>			Infrastructure Event Management (Available for additional fee)	Infrastructure Event Management (Included)
<b>Programmatic Case Management</b>			AWS Support API	AWS Support API
<b>Third-Party Software Support</b>			Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting
<b>Account Assistance</b>				Assigned Support Concierge
<b>Proactive Guidance</b>				Designated Technical Account Manager

Figure 28: Day1 Support Level Details

**Day1's SaaS offering with Infor:** Purchasing Entities may contact Infor Xtreme Support at any time by submitting an incident via the Infor Xtreme® Portal located at [www.infor.com/inforxtreme](http://www.infor.com/inforxtreme) or by placing a call during Infor's scheduled business hours. For a complete listing of the Xtreme Support phone numbers, access the "Contact Us" option under the "About" section on the home page of the Infor Xtreme® Portal at [www.infor.com/inforxtreme](http://www.infor.com/inforxtreme). Infor encourages online entry of incidents—a method that enables Infor Support analysts to quickly begin analyzing the issue. Online access also provides 24x7 access to a variety of online support tools. Online access can be requested from the Licensee's designated Contact Administrator or by contacting the Infor Customer Care team. In addition to logging a new incident through the Infor Xtreme® Portal, the Licensee has access to other Support services and capabilities, including:

- Ability to view and update Licensee's incident history and status
- Access to the Xtreme Support Knowledge Base
- Access to Frequently Asked Questions (and responses)
- Access to the latest information about new product releases
- Ability to participate in Infor Xtreme Communities to share best practices and resolutions to business challenges with other Licensees
- Access to analytics providing information on incidents, customer satisfaction, Knowledge Base usage, and Designated Contact(s)
- In order for Infor to effectively address an incident, Purchasing Entities should have the following information readily available when logging an incident via the Infor Xtreme® Portal or placing a call. Doing so will help us respond in a more effective and timely manner:
  - Infor customer number and contact details (name, email address, and contact phone number).
  - Details of the incident (e.g., error messages and how to reproduce the error). If Purchasing Entities are logging via the Infor Xtreme® Portal, include screen shots and output examples.
  - Description of the issue's frequency and predictability (e.g., intermittently, each time function is used, etc.)
  - Description of the issue's impact (e.g. Does it impact all users? Does it occur on all PCs/workstations?)
  - For Service requests, a description of the request and time frame for which Purchasing Entities would like to have the request executed.

**Infor Cloud Roles and Responsibilities:** The following is a high level guideline for roles and responsibilities in the implementation, operation, and ongoing Support of Infor Cloud Solutions. Detailed Roles and Responsibilities are available for many of Infor's Cloud solutions and documented in a Knowledge Base on the Infor Xtreme® Portal.

Implementation Tasks	LICENSEE	INFOR
Project management and implementation assistance per Services Agreement and/or Work Order, if executed		✓
Management of implementation, integration, and extension related tasks	✓	
End-user training	✓	
Functional testing of all purchased modules and processes	✓	

Implementation Tasks	LICENSEE	INFOR
<b>Incident Management</b>		
Creation and management of users on the Infor Xtreme® Portal	✓	
First level user support of Xtreme incident	✓	
Incident escalation management		✓
Troubleshoot issues with Infor Subscription Software products when Licensee experiences unexpected results		✓
<b>Life Cycle Management</b>		
Provide Subscription Software updates that include fixes for incidents and minor and major releases		✓
Install patches/upgrades to OS and application environment		✓
Functional testing of Fixes, Patches, Upgrades		✓
<b>Change Management</b>		
Request changes to product configuration	✓	
Execute customer approved changes following change management process		✓
<b>System Administration</b>		
Deployment and management of system security		✓
Maintain file systems and directories, such as: purge user reports		✓
Monitor drive/file system space		✓
Monitor system and applications		✓
Monitor and administer operating system functions		✓
Maintain and manage logs within the environment and application		✓
Maintain middleware components		✓
Management of application	✓	
Management and authorization of users	✓	
<b>Backups</b>		
Perform and maintain backups		✓
Data copy and restores at client's request		✓
<b>Database Administration</b>		
Performance tuning of databases		✓

Implementation Tasks	LICENSEE	INFOR
Database administration		✓
<b>Solution Support</b>		
Provide assistance and interpretation of error messages		✓
Clarify program functionality and system capabilities		✓
Assist with interpretation of system documentation		✓
Interactive/recorded Support Briefings		✓
Knowledge Base (KB) article creation and maintenance		✓

Figure 29: Infor Cloud Roles and Responsibilities

#### 1.12.4 Consequences for Not Meeting SLA Standard for Response Time and Incident Fix Time [RFP 8.12.4]

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

Please refer to Section 1.12.2 Standard Uptime [RFP 8.12.2].

**Day1's SaaS offering with Infor:** Infor's Response targets are described in the table below.

<b>Enhanced Response Targets Severity 1 (Production System Down)</b>	Infor will make commercially reasonable efforts to respond to Severity 1 incidents within 30 minutes during scheduled business hours.  <b>Note:</b> All Severity 1 issues which occur outside of standard Xtreme Support hours must be reported by telephone to the local Infor Xtreme Support Center.
<b>All other Severities (except 5)</b>	Infor will make commercially reasonable efforts to respond within one (1) business hour during scheduled coverage hours.

Figure 30: Infor Response Targets

#### 1.12.5 Planned Downtime [RFP 8.12.5]

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

Day1 asserts that through the use of AWS and a robust cloud architecture, there is never a need to have a planned downtime from the IaaS perspective. However, we understand that as Purchasing Entities start to use our cloud solutions, their existing systems may require planned downtime. Day1 and NASPO customers will define a list of responsible POCs for planned downtime in order to develop the appropriate procedures and schedule. Day1 will communicate with defined personnel for all planned downtime. And schedules can be tailored to some extent to

support individual customer needs with some limitation when deviating from best practices. The key elements for scheduled downtime include:

- Developing communications to users
- Assessing criticality of system for downtime
- Developing a schedule for downtime
- Understanding acceptable downtime hours and duration
- Identifying notification periods
- Identifying stakeholders involved with scheduled downtime

**Day1's SaaS offering with Infor:** There are minimal scheduled downtimes for maintenance of the applications; customers' designated contacts are notified beforehand through Infor Xtreme. Infor's goal is to provide access to the services at Infor's Internet gateway(s) twenty-four hours per day, seven days a week, except during Scheduled Maintenance. Infor's service level objective is 99.5% Availability measured on a monthly basis.

Infor maintains consistency across the multiple solutions and services where ever possible, but there are some areas that differ due to the nature of various markets being served and/or the technical requirements of a solution. Although there are multiple opportunities for maintenance windows, the number of windows taken is minimized as much as possible and announced at least 72 hours in advance, unless there is an emergency. All times are in the local time of the region where the application is deployed as noted below. For example, maintenance window times for solutions being served by US-East are in Eastern US Time.

	Maintenance Window Opportunities	Normal Maintenance Frequency	Disaster Recovery
<b>EAM</b>	Friday and Sunday 12:00 AM until 2:00 AM	Once a month	RPO < 1 hour RTO < 1 hour
<b>Business Intelligence</b>	Friday 12:00 AM until 2 AM	Once a month	RPO, RTO Near 0
<b>CloudSuite Business / Industrial</b>	Friday and Saturday 12:00 AM until 2:00 AM	Once a month or less	RPO < 5 minutes RTO < 5 minutes
<b>SyteLine 8.x</b>	Friday and Sunday 12:00 AM until 2:00 AM	Once a month or less	RPO/RTO < 1 hour
<b>Expense Management</b>	Friday and Sunday 12:00 AM until 2:00 AM	Once a month	RPO, RTO Near 0
<b>Hosted Health Information Exchange</b>	Sunday 12:00 AM until 8:00 AM	Once a month	RPO < 15 minutes RTO 48 hours
<b>HRSD</b>	Friday 12:00 AM until 8:00 AM	Once a month	RPO, RTO Near 0
<b>Hospitality Management Solution</b>	Thursday 3:00 AM until 5:00 AM	Once a month	RPO, RTO Near 0
<b>Infor Reporting</b>	Sunday 12:00 AM until 8:00 AM	Once a month	RPO, RTO <i>tbd</i>

	Maintenance Window Opportunities	Normal Maintenance Frequency	Disaster Recovery
Infor Learning Management	Sunday 12:00AM until 8:00 AM	Once a month	RPO, RTO Near 0
Mingle CE	Tuesday 12:00 AM until 2:00 AM	Once a month	RPO, RTO <i>tbd</i>
ION CE	Tuesday 12:00 AM until 2:00 AM	Once a month	RPO, RTO <i>tbd</i>
Infor Enterprise Search (IES)	Friday and Sunday 12:00 AM until 2:00 AM	Once a month	RPO, RTO <i>tbd</i>
Marketing Resource Management	Sunday 12:00 AM until 8:00 AM	Once a month	RPO, RTO <i>tbd</i>
Talent Management	TBD	Once a month, third Sunday	RPO, RTO Near 0
Talent Science	TBD	Once a month, third Saturday	RPO, RTO Near 0
AMSI/eSite	Sunday 9:00 PM until 11:00 PM	Once a month or less	RPO/RTO < 5 minutes

Figure 31: Infor Maintenance Window Times

### 1.12.6 Consequences for Not Meeting SLA Standard for Disaster Recovery [RFP 8.12.6]

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

In the event of failure to deliver Disaster Recovery SLAs, Service Credit shall be applied in lieu of liquidated damages against the following year of service cost. If service is discontinued for any reason, the Service Credit shall be in the form of a rebate at the end of service. If service is discontinued for any reason, the Service Credit shall be in the form of a rebate at the end of service. Service Credits shall be computed by dividing the number of Days of Service credited by the number 365 and multiplied by the Annual Service Fee. This will be negotiated with each NASPO customer environment. Please refer to *Section 1.12.2 Standard Uptime [RFP 8.12.2]* for additional clarification.

**Day1's SaaS offering with Infor:** The consequences/remedies for failure to meet disaster recovery metrics appear below.

Availability	Service Level Credit
99.500% or greater	No Service Level Credit
99.499% - 99.000%	5% of the monthly prorated subscription fee
98.999% - 98.500%	15% of the monthly prorated subscription fee
98.499% - 95.000%	25% of the monthly prorated subscription fee
Below 95.000%	35% of the monthly prorated subscription fee



Figure 32: Disaster Recovery SLAs

### 1.12.7 Sample Performance Reports [RFP 8.12.7]

*Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.*

Day1 can provide Purchasing Entities with performance reports of their cloud infrastructure through multiple different channels to include inherent AWS tools such as CloudWatch, and third party tools such as Monitis. A brief description of such applications, as well as screenshots of possible reports have been provided below. The following report samples are available online and can be customized in a customer dashboard. They can be delivered as real-time or batch statistics. To protect the privacy of our current customers' samples have been sanitized.

<b>Monitis</b>	Monitis is used for external uptime monitoring of cloud resources. This tool determines if a cloud resource is reachable from the internet using multiple protocols, such as HTTP, HTTPS, PING, and DNS. It scans in 1 minute monitoring intervals and has a 2 year historical archive.
<b>Amazon CloudWatch</b>	Amazon CloudWatch provides monitoring services for AWS cloud resources and for applications that run on AWS. Day1 can provide Purchasing Entities with access to CloudWatch reports where they can view performance metrics such as EC2 CPU utilization, data transfers, disk usage, etc.
<b>FreshDesk</b>	FreshDesk covers all ticketing and engineering resource management. Escalation policies and SLAs are used to intelligently distribute tickets to appropriate engineering resources. FreshDesk also serves as a customer portal for not only for service requests, but shared documentation.
<b>Cloud Defender</b>	Cloud based security suite includes intrusion detection, web applications firewall, compliance management, and managed security analytics modules. Ability to build SOC based custom dashboards and report on required metrics to ensure compliance to predefined standards or custom built.
<b>Cloud Insight</b>	Cloud centric configuration and vulnerability management tool. Ability to create custom dashboards and report on the security health of customer environments.
<b>Scalr</b>	Scalr monitors Cloud resources and aggregates monitoring data from other toolsets. It allows the creation of customized dashboards showing critical health information of the cloud environment, policy based automation and reporting of defined health and operational metrics. It includes a full cost management module with customer dashboards for independent live review.

Figure 33: Day1 Cloud Reporting Tools

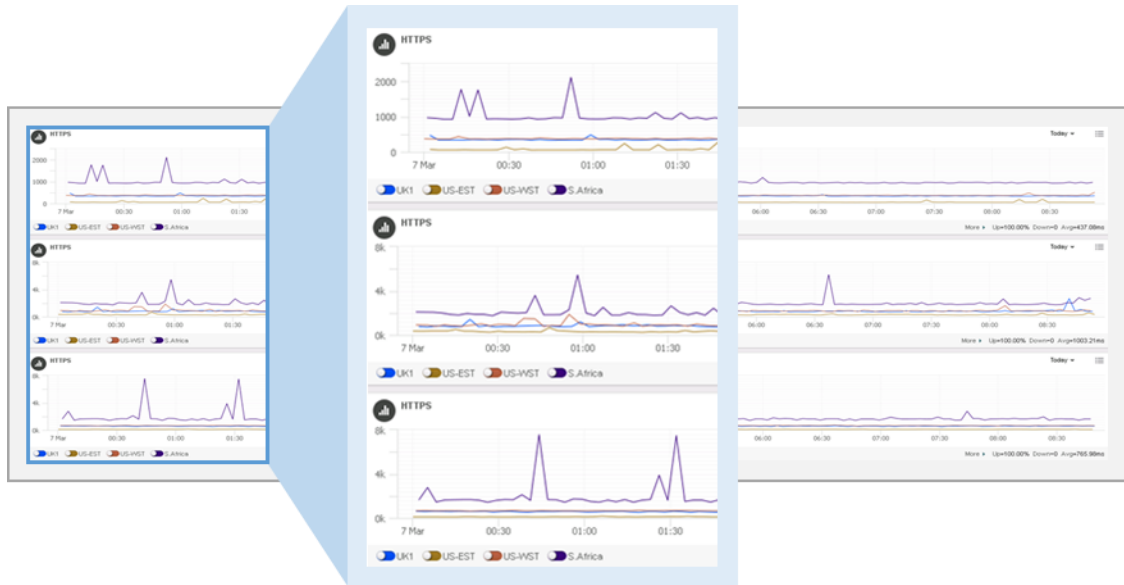


Figure 34: Sample Report #1

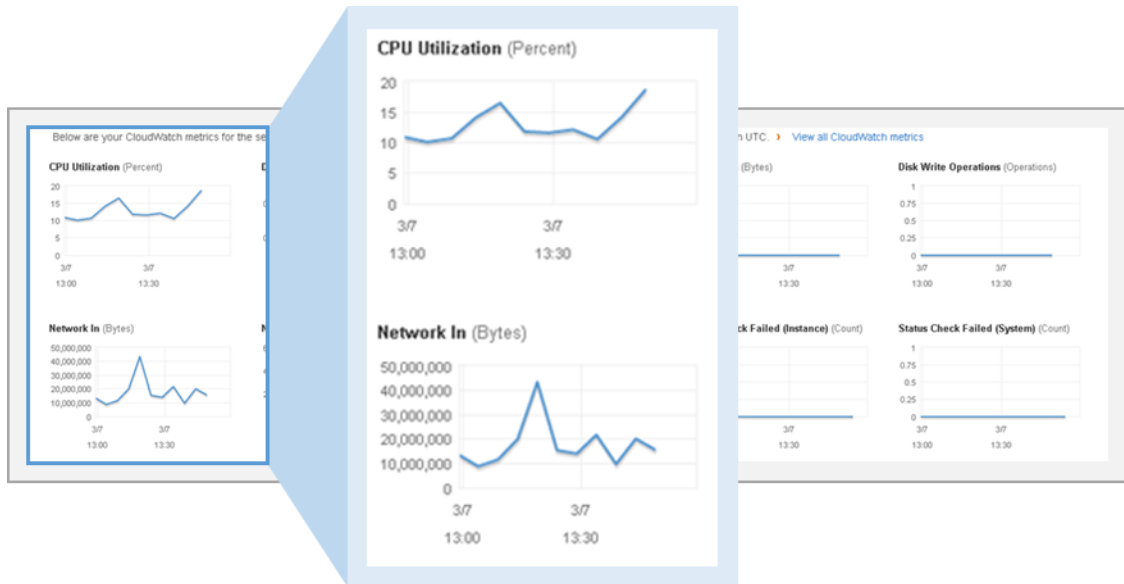


Figure 35: Sample Report #2

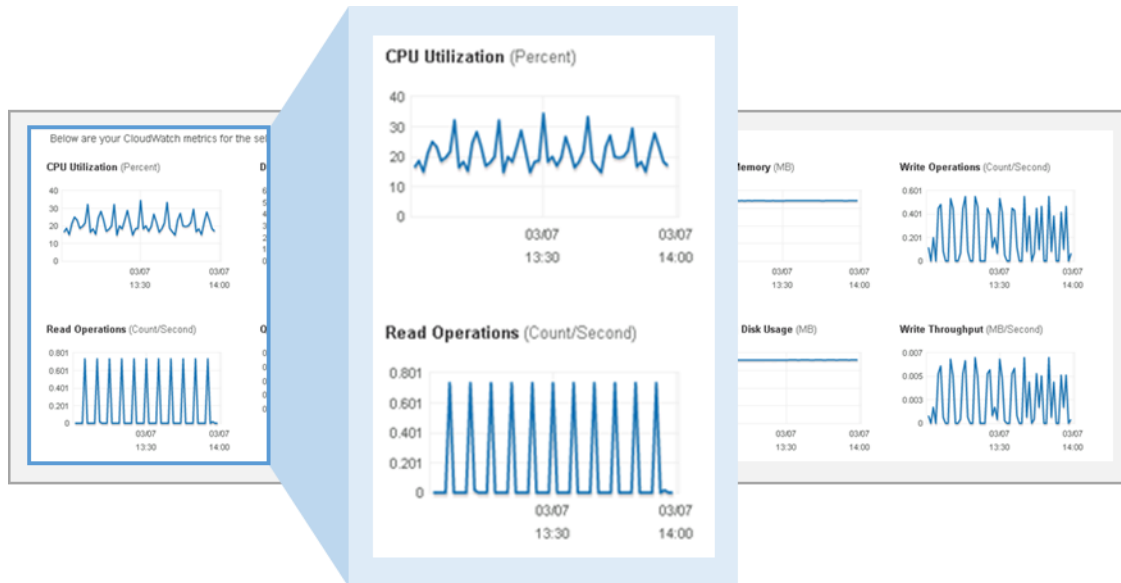


Figure 36: Sample Report #3

### 1.12.8 Report Printing [RFP 8.12.8]

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

Day1's monitoring and reporting modules have built-in support for historical, statistical, and usage reports. Day1 also supports cost management review and can provide real-time reporting and suggestions for managing AWS spend. These abilities can be extended to customers in the form of customized dashboards for independent review. NASPO Participating Entities will have the ability to print reports locally or have periodic reports sent via electronic means. Reports can be provided in a multitude of ways to include Microsoft Excel, or Adobe PDF depending on the report type.

### 1.12.9 On-Demand Deployment [RFP 8.12.9]

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

The On-Demand services as described in *Section 1.1.2.5 Measured Services [RFP 8.1.2.5]* are made accessible to all NASPO purchasing entities 24x365 and accessible through means as described in *Section 1.1.2.2 Broad Network Access [RFP 8.1.2.2]*.

### 1.12.10 Scale-up and Scale-Down [RFP 8.12.10]

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

The auto-scaling features as described in *Section 1.1.2.4 Rapid Elasticity [RFP 8.1.2.4]* are made accessible to all NASPO purchasing entities 24x365 and accessible through means as described in *section S.1.2.2 Broad Network Access [RFP 8.1.2.2]*.

**Day1's SaaS offering with Infor:** Infor employs AWS ELBs and autoscaling to help maintain application availability; we also use EC2 clustering as a fault tolerant measure.

### 1.13 (E) Cloud Security Alliance Questionnaires [RFP 8.13]

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

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

Day1 asserts that our solutions are compliant with Level 1 CSA STAR Registry Self-Assessment. Please see the attached CSA STAR Self-Assessment documents.

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](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.

**Day1's SaaS offering with Infor:** Infor does align to the Cloud Security Alliance standards, and is in the process of completing the CSA Star Self-Assessment for our multi-tenant environment. Our CSA assessment for our single-tenant environment is attached. Please see the attached CAIQ document, provided in the Appendices. After successful completion of CSA STAR Attestation, Infor will pursue completion of this certification tier.

### 1.14 (E) Service Provisioning [RFP 8.14]

Day1's approach to service provisioning focuses on the entities individual needs and preferences. We offer the ability to interface entirely online – selecting, purchasing, provisioning, and de-provisioning services; migrating to and from the cloud; and engaging customer support – through our [www.day1solutions.com/NASPO](http://www.day1solutions.com/NASPO) website portal and the AWS Management Console. We also encourage telephone and face-to-face service requests either through our assigned project managers or our 24/7 live customer support call center as part of our Managed Services desk. Upon award, we will implement a toll free phone number. Regardless of the mechanism used to request service, participating entities can track and monitor requests in real time through our built-in customer service portal. During the participating addendum period, entities can select and define varying levels of dedicated service (to be defined in our SLA) that allow for online self-help, online support and telephone based Help Desk services, or contracted custom support services.

**Provisioning and De-Provisioning** - When entities choose facilitated provisioning services, we will engage the entity CIO, GIO, and other technical representatives to understand the hosting needs and overall Cloud strategies; identify alternative migration strategies and ROI; develop solution architectures meeting current and forecasted future usage and performance requirements; establish low-risk migration strategies to ensure continuity of operations; and facilitate the migration to hosted solutions. Alternately, self-provisioning of select services will be available, through the AWS Management Console. Entities may engage as desired with the Day1 PMO or their designated project manager to determine which approach is best suited for a given need. Similar to our provisioning customer service, entities may de-provision established services through the AWS Management Console or engage their project manager to facilitate de-provisioning of a wider range of cloud services.

#### 1.14.1 Emergency/Rush Service Implementation [RFP 8.14.1]

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

As described above, Day1 offers instant self-provisioning of select services through the AWS Management Console. If pre-approved via an open purchase order, the order will instantly provision on the cloud and the user will be notified via email when it is ready.

It is important to note that assisted or service-integrated rush services are also available for more comprehensive or complex service needs. Following predefined procedures adapted to each entity's provisioning processes, project managers and customer service teams (Managed Services) are trained to quickly respond to rush and emergency service requests. These procedures will define what services can be offered for rapid deployment, alternatives for rapid deployment, facilitated steps for high-priority and resolution, and reporting resolution times.

**Day1's SaaS offering with Infor:** Infor's Xtreme Support is available 24x7x365; however, Infor's standard lead time is 48 hours. If there were a rush implementation of a security patch Infor would do everything commercially viable to push a patch or bug fix as soon as the Cloud Operations team gives the approval.

#### 1.14.2 Lead-Time for Provisioning [RFP 8.14.2]

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

Day1 is an authorized reseller of AWS. Through the use of the AWS Management Console, authorized users for each entity will be able to provision cloud services directly from AWS. Most services can be provisioned to the cloud in 15 minutes or less with no lead-time, available with a preauthorized open purchase order.

Additionally, our assisted provisioning services will be quickly provided according to lead-times defined in the participating addendum SLA, with a business day or less lead-time available for rapid deployment. These requests and response times will be monitored for continuous process improvement that will include additional training measures, additional automated provisioning tools, and upfront planning, each working to reduce service times in emergencies.

**Day1's SaaS offering with Infor:** Infor's standard lead time is 48 hours.

## 1.15 (E) Back Up and Disaster Plan [RFP 8.15]

### 1.15.1 Methodologies for Backup and Restore Services [RFP 8.15.1]

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

As stated in *Section 1.5.3 Accessing Purchasing Entity's user accounts and data [RFP 8.5.3]* Day1 does not access customer data and as part of the *Figure 22: AWS Shared Responsibility Model* the customer manages their own data. As a result, Day1 does not apply legal retention periods or disposition of a Purchasing Entities' data.

**Day1's SaaS offering with Infor:** Infor's SaaS multi-tenant cloud hosted environment offers a standard retention period of 90 days. If a US government agency requires access to data either indirectly or directly, then that entity must follow due course of action specified in the US Patriot Act requiring they perform accepted legal practices to include gaining court permission. Infor only releases customer information when a formal court order is presented or upon end of contract / termination.

### 1.15.2 Inherent Disaster Recovery Risks [RFP 8.15.2]

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

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. As NASPO begins the adoption of cloud based services, there are major considerations for its DR objectives. Our consultants have specific experiences with developing cloud based DR capabilities and can guide NASPO purchasing entities in developing an approach to DR that best meets the requirements of the organization. For example, the cloud provides NASPO with the flexibility of implementing DR through "backup & restore," "pilot light," "warm standby," and "multi-site" configurations. A brief explanation of the different types of DR are explained below:

#### **Backup and Restore**

This DR method is usually the easiest to adopt as it mimics a traditional IT environment. In most traditional environments, data is backed up to tape and sent off-site regularly. To support this type of DR requirement with AWS, Day1 may leverage backups to an Amazon Simple Storage Service (S3) bucket. Using Amazon S3 is ideal for backup data, as it is designed to provide 99.99999999% 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. Additionally, Day1 can support the use of AWS Storage Gateway, where NASPO customers can automatically back up on-premises data to Amazon S3.

#### **Pilot Light**

In this scenario Day1 will guide the NASPO customers in understanding the most critical components of their system. These core components will be pre-configured and waiting in sedentary state in the cloud. This scenario is similar to the Backup and Restore scenario This scenario is analogous to a backup and restore scenario; however, NASPO customers must ensure that they have the most critical core elements of their system already configured and running in AWS (the pilot light). When the time comes for recovery, NASPO would execute

	the DR plan which rapidly provisions a full-scale production environment around these components.
<b>Warm Standby</b>	In a Warm Standby DR scenario, a scaled-down version of the fully functional environment is always running in the cloud. It decreases recovery time as some services are always running. By identifying business-critical systems, customers could fully duplicate these systems on AWS and have them always on.
<b>Multi-site Solution</b>	A multi-site solution will run in the cloud as well as on existing on-premise infrastructure in an active-active configuration. During a disaster situation, traffic would simply be re-routed to the cloud based instances, which can scale to handle the full production load.

Figure 37: Disaster Recovery Definitions

Day1 understands that there are inherent risks associated with Disaster Recovery (DR). These risks include additional costs, capacity planning, replication failure, loss of data, management of multiple environments, etc. With AWS, NASPO customers can eliminate the majority of these risks such as 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. The following table provides an overview of the advantages of using AWS for DR as opposed to traditional on-premise DR approaches:

Traditional DR/COOP and Backup Requirements and Issues	AWS Capabilities for DR / COOP / Backup Solutions
<ul style="list-style-type: none"> <li>• Facilities to house additional infrastructure, including power and cooling.</li> <li>• Security to ensure the physical protection of assets.</li> <li>• Suitable capacity to scale the environment.</li> <li>• Support for repairing, replacing, and refreshing the infrastructure.</li> <li>• Contractual agreements with an Internet Service Provider (ISP) to provide Internet connectivity that can sustain bandwidth utilization for the environment under a full load.</li> <li>• Network infrastructure such as firewalls, routers, switches, and load balancers.</li> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• Fast Performance: Fast, disk-based storage and retrieval of files.</li> <li>• No Tape: Eliminate costs associated with transporting, storing, and retrieving tape media and associated tape backup software.</li> <li>• Compliance: Minimize downtime to avoid breaching Service Level Agreements (SLAs).</li> <li>• Elasticity: Add any amount of data, quickly. Easily expire and delete without handling media.</li> <li>• Security: Secure and durable cloud DR platform with industry-recognized certifications and audits.</li> <li>• Partners: AWS solution providers and system integration partners to help with deployments.</li> </ul>

Figure 38: AWS DR/COOP/Backup Capabilities

**Day1's SaaS offering with Infor:** Infor is not aware of inherent risks in our DR plan and will proactively monitor for any potential future risks that may be identified.

**1.15.3 Multi Data Center Infrastructure Support [RFP 8.15.3]**

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

The AWS cloud infrastructure is built around AWS Regions and Availability Zones where a region is described as a geographical area where AWS has multiple Availability Zones. AWS Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. Availability Zones are all redundantly connected to multiple tier-1 transit providers. These Availability Zones offer NASPO purchasing entities with the ability to operate IT environments that are more fault tolerant, highly available, and scalable than would be possible from a single data center. AWS currently has 12 regions and 32 Availability Zones throughout the world: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), South America (Sao Paulo), and China (Beijing). Figure 39 below depicts the current AWS regions and number of Availability Zones in each Region, along with new regions that are coming soon.

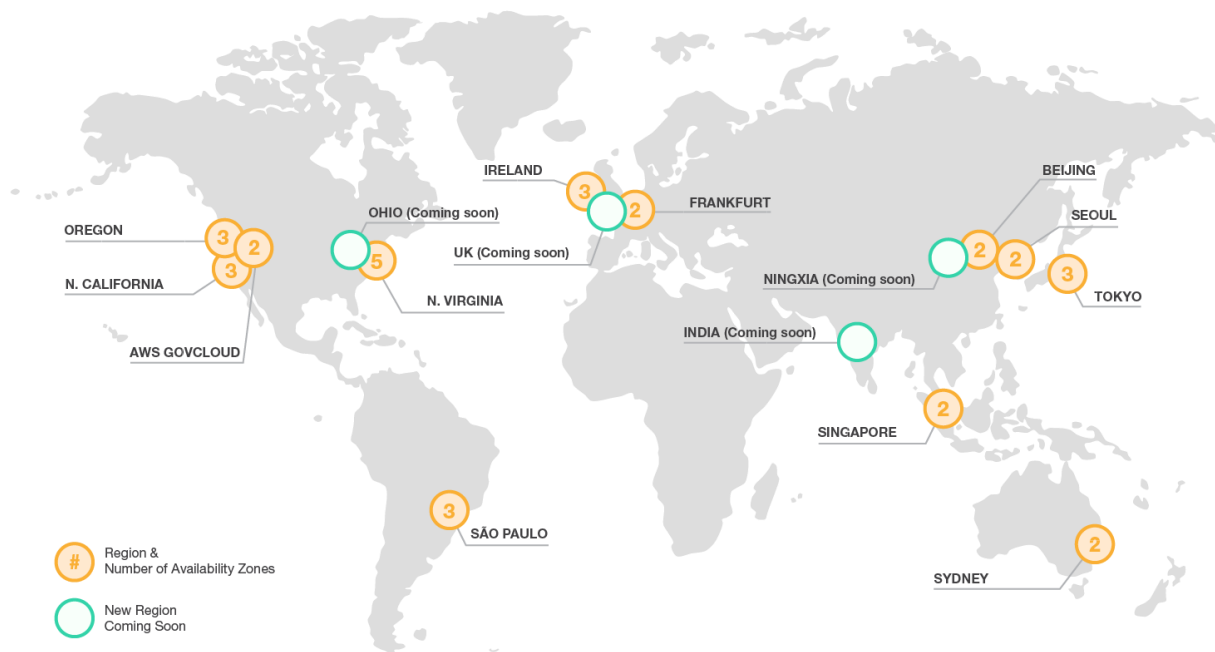


Figure 39: Global Map of AWS Regions and Edge Locations

Day1 can support and certify that all data contained within AWS are guaranteed to stay within the United States by only offering AWS services specific to Regions and Availability Zones within the United States to include US East (Northern Virginia), US West (Oregon), US West (Northern California), and AWS GovCloud (US) (Oregon).



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.

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 purchasing entities with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). Please refer to *Section 1.15.3 Multi Data Center Infrastructure Support [RFP8.15.3]* for additional information on AWS Regions and Availability Zones.

**Day1's SaaS offering with Infor:** As illustrated above, AWS provides multiple Availability Zones (AZ) that provide redundancy and enable failover capabilities. Infor employs AWS ELBs and autoscaling to help maintain application availability; we also use EC2 clustering as a fault tolerant measure.

**AWS MIGRATION & HOSTING EXPERIENCE**

Day1 Solutions supported Hawaii's Office of Information Management and Technology in an effort to retire aging infrastructure and migrate over 25 websites to AWS to increase citizen engagement and provide additional enhancements in future web-based services.

## 1.16 (E) Solution Administration [RFP 8.16]

### 1.16.1 Managing Identity and User Accounts [RFP 8.16.1]

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

The AWS Management console can be used by NASPO purchasing entities to access and manage all AWS resources through a simple and intuitive web-based user interface secured through Secure Socket Layers (SSL) encryption. Day1 recommends the use of AWS Multi-Factor Authentication (MFA) to secure access to NASPO purchasing entity AWS resources. AWS MFA is a simple best practice that adds an extra layer of protection on top of a typical user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for a user name and password (the first factor—"what you know"), as well as for an authentication code from an AWS MFA device (the second factor—"what you have").

Additionally, Day1 will help to implement Identity and Access Management (IAM) to control access to NASPO purchasing entity AWS specific services and resources. This will ensure that only users approved by NASPO have the ability to access the internal IT resources. Please see *Section 1.6.7 Visibility Restrictions [RFP 8.6.7]* for more information on IAM.

### 1.16.2 Anti-Virus Protection [RFP 8.16.2]

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

In support of the shared responsibility model *Figure 22: AWS Shared Responsibility Model*, Day1 can help to educate and inform NASPO purchasing entities on the AWS Shared Responsibilities model as described in *Section 1.5.1 Data Protection [RFP 8.5.1]*. Day1's professional services and managed services team can help to implement a wide variety of applications for NASPO Purchasing Entities cloud based environments to provide greater control over services categorized as "Customer" responsibility in the shared model. This includes the installation, and implementation of anti-virus protection at the data store level. While this may be a customer responsibility

### 1.16.3 Data Migration [RFP 8.16.3]

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

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.

Day1 has identified AWS Import/Export as a data migration tool to move large amounts of data into and out of AWS. AWS Import/Export allows for movement of large volumes of data using portable storage devices for transport. Day1 can help NASPO transfer data to AWS directly using storage devices and Amazon's high-speed internal network and bypassing the Internet. For significant data sets, AWS Import/Export is often faster than Internet transfer and more cost effective than upgrading existing connectivity. With Import/Export encryption is mandatory, and AWS will encrypt data using the password they specified and transfer it onto the device

### 1.16.4 Administering the Solution [RFP 8.16.4]

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

As described in *Section 1.17.1 Cloud hosting Provisioning Process [RFP 8.17.1]*, Day1 has implemented a "single pane of glass" tools at multiple customer sites to simplify administration of differing customer environments. This helps to provide consistency in monitoring disparate infrastructures and allows our team to manage the solution in a distrusted manner. Our team will leverage a "single pane of glass" tool that most adequately meets the support and administration requirements of NASPO purchasing entities. This will provide NASPO with a single perspective of administration, ordering and monitoring. The specific tools of choice would include:

- Ostrato
- Rightscale
- DivvyCloud

### 1.16.5 Defined Administration Policies [RFP 8.16.5]

*Ability to apply participating entity defined administration polices in managing a solution.*

Access to a participating entities AWS account will be controlled by the participating entity's person-in-charge. We will work with each entity to apply administrative policies at the group and user level to ensure specific controls and

security features related to their account. Access to different functions within AWS can be controlled down to the user level, including, but not limited to, restricting who can, increase/decrease cloud resources like storage or compute, provision new services, change points of contact, access billing information, and much more. Because each participating entity is contained within an independent and isolated account, the resources that the entity provisions in those accounts can be managed with entity defined administration policies.

Adopting new or integrating existing Identity Access Management (IAM) solutions can federate and provide single-sign-on functionality to AWS as well as the cloud instances themselves (e.g. RDP, SSH, VPN, etc.), and application-level services (e.g. SaaS application log-in, REST web service end-points, etc). Day1 has experience working hand-in-hand with current WSCA customers in defining administrative policies based on their needs. We are confident that our combination of experience, security and IT administration subject matter expertise, and industry-leading cloud infrastructure providers will quickly satisfy IT managers of participating entities' requests for administrative configurations.

## 1.17 (E) Hosting and Provisioning [RFP 8.17]

---

### 1.17.1 Cloud hosting Provisioning Process [RFP 8.17.1]

---

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

Day1 understands that this program may require precise provisioning process, order management, and billing controls for NASPO and potential NASPO purchasing entities. Please refer to the AWS Management Console in *Section 1.17.2 Provided Tool Sets [RFP 8.17.2]* to understand how NASPO purchasing entities may quickly provision resources.

In order to ensure a timeline and controlled provisioning process that Day1 leverages may leverage custom tools and home grown processes to monitor the resources and account for possible billing needs. We will work closely with NASPO to understand the needs for order management and provisioning to assure that we provide a solution specific to the needs of the participating entities. We have domain knowledge and understanding with multiple tools and will provide guidance towards a specific tool depending on the specific use case. Depending on the needs of NASPO, Day1 may implement tools, which are often referred to as a "single pane of glass" tool to provide consistency in monitoring disparate infrastructure components. They can provide NASPO with a single perspective on ordering and monitoring of deployment. These would include tools such as:

- Orbitera
- Ostrato
- Rightscale
- DivvyCloud

While these tools provide the "single pane of glass" for provisioning and order management, they may do so with some compromises in technical capabilities. They are often best suited if order management of infrastructure components may expand outside the control of IT. Day1 will work with NASPO to understand the order management requirements of NASPO and its customers and make recommendations based on our findings. Day1 will focus on a goal of working with NASPO to develop an order management policy that enables control over infrastructure components being deployed without compromising requirements of NASPO and customers. For example, in order to take full advantage of the AWS API's and applications, Day1 may suggest the use of the AWS Management Console

to control order management. While it may not provide the same “single pane of glass,” the use of the AWS Management Console for order management requires minimal sacrifices in deploying AWS specific tools.

Day1 uses a combination of tools to provide a comprehensive management of usage and billing. While the AWS management console facilitates cloud management including monitoring monthly spending by service, and managing security credentials, it provides only basic usage information. Day1 leverages Orbitera to provide sophisticated usage, and on-line billing reports. Depending on the requirements of NASPO, we may leverage tools such as the AWS management console or employ sophisticated tools like Orbitera. Using Orbitera, Day1 can provide usage reports based on the specified level of information required to meet the needs of NASPO purchasing entities. We will work with NASPO and customers to identify the appropriate users who need access to these reports and provide those users with specific accounts and/or privileges required to view the reports. Dashboard views of usage reports can be specifically provided for designated users. Day1 will make these usage reports available to NASPO quickly and as needed. NASPO may require an entirely customer service centric approach to billing, we make recommendations for optimizing performance, enhancing security and data privacy, enabling features, and standardizing billing for customers and project teams.

**Day1's SaaS offering with Infor:** Infor follows a pre-defined / tested provisioning process for CloudSuites that consists of a combination of cloning golden images, bootstrapping and creating tenants using a pre-defined REST API. A provisioning recipe is pre-defined and tested for each CloudSuite and its various bundles consisting of optional products. When a customer purchases a CloudSuite the provisioning recipe is executed to create the customer's environment.

### 1.17.2 Provided Tool Sets [RFP 8.17.2]

*Provide tool sets at minimum for:*

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

Day1 will provide NASPO purchasing entities with access to multiple tools and methods for hosting and provisioning AWS resources to include the AWS Management Console, AWS Command Line Interface (CLI), and even existing on-premise management tools. NASPO purchasing entities can use the AWS Management Console as a single destination for managing all AWS resources to perform a number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console can also enable NASPO purchasing entities with the ability 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.

In addition, the AWS Management Console (as seen in Figure 40 below), NASPO purchasing entities can use AWS CLI as a unified tool for managing AWS cloud services. With just one tool to download and configure, NASPO customers can control multiple AWS resources from the command line and automate them through custom developed 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).

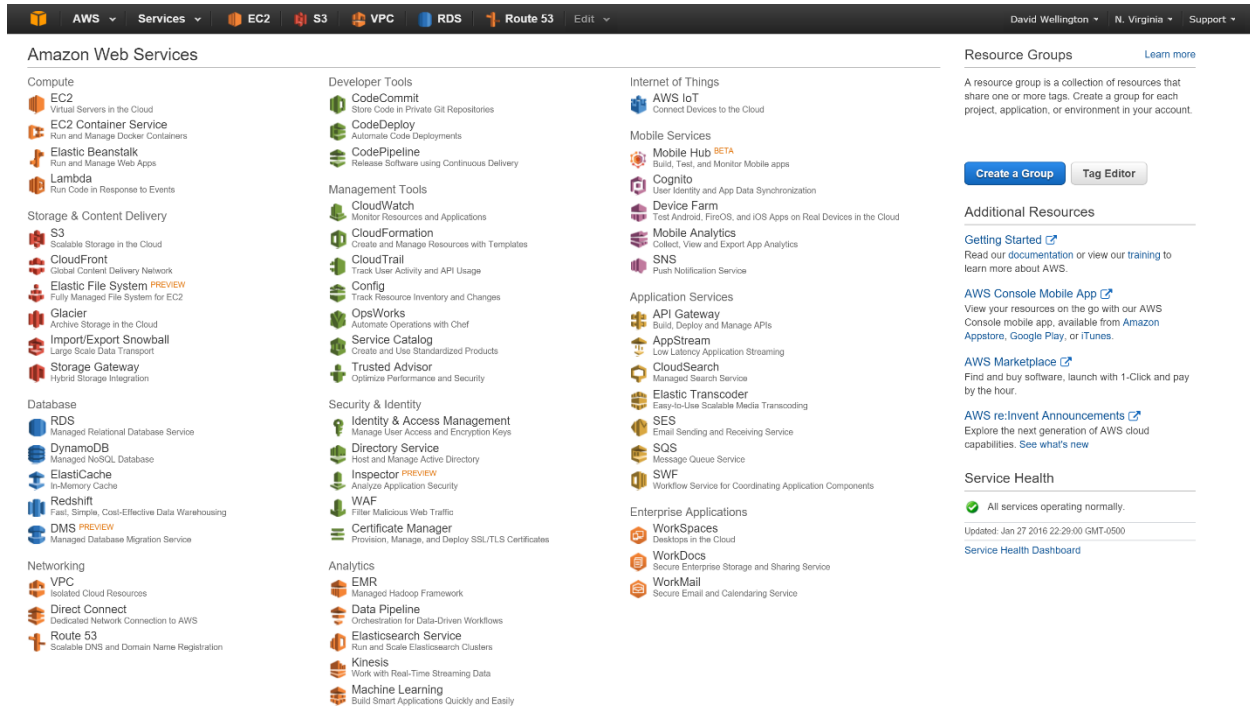


Figure 40: The AWS Management Console

Many of the tools that organizations use to manage on-premises environments can be integrated with AWS as well. Day1 understands that integrating an AWS environment can provide a simpler and quicker path for cloud adoption, reducing the need for operations team to learn new tools or develop completely new processes. The examples below provide context as to how Day1 can help integrate existing on-premise tools with AWS:

- AWS Management Portal for VMware 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. This provides 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.

**Day1's SaaS offering with Infor:** In the Infor Cloud, Infor will determine (with the help of the customer) the best configuration for the customer's requirements. However, for the basis of this response, we have assumed a multi-tenant environment whereby Center for Internet Security (CI Security) benchmarks are followed.

Infor has partnered with AWS, the world leader in Cloud IAAS / PAAS, for its cloud offering. Infor deploys all its infrastructure on AWS and uses AWS features like EBS Snapshots and AMI's to create / store golden images of its environments. These AMI and snapshots are combined with extensive use of bootstrapping scripts to create environments using a REST API.

Infor maintains, in an immutable location, a centralized SIEM tool to centrally store, manage, and analyze log data.

## 1.18 (E) Trial and Testing Periods (Pre- and Post-Purchase) [RFP 8.18]

---

### 1.18.1 Testing and Training Periods [RFP 8.18.1]

---

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

Day1 will review testing timelines and training programs with NASPO customers per opportunity. Building customer success is defined by each unique relationship and will be established after assessment of needs. Day1 offers on-going platform training for customers at no additional cost based on the managed services support tier. We will work together with customers to understand their existing environment and guide them through migration to ensure customer success first and foremost. Additionally, for customers new to AWS or using AWS Marketplace Day1 can make available multiple trial software options. AWS Marketplace offers free trials and hourly and monthly pricing models. Customers can get started with software free trials or AWS Free Tier Eligible Software.

**Day1's SaaS offering with Infor:** Infor has a large training department that consists of multiple avenues to work on and learn about our products: onsite classes, offsite classes, web based, online library, one-on-one for super users, etc. Through our training department our customers can learn how to use and manage the Infor applications however is best for them. Additional content regarding our training programs appear below.

### 1.18.2 Test and POC environments [RFP 8.18.2]

---

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

Day1 is ready to make AWS Free Tier available to NASPO purchasing entities as a way to test AWS products and services prior to purchase. The AWS Free Tier can be leveraged by NASPO customers for a 12 Month Introductory Period and is only available to new AWS customers, and is only available for 12 months following initial AWS sign-up date. Day1 has guided new customers through the use of AWS Free Tier as a precursor to purchasing AWS services. Often, Day1 customers find AWS Free Tier has a handy tool to understand how products will be integrated into their environment and as a proof of concept prior to purchase. A full list of products and services that can be at <https://aws.amazon.com/free/>.

































solutions as seen in *Section 1.19.1 Service Integration [RFP 8.19.1]* and *Section 1.19.2 Customize and Personalize Solutions [RFP 8.19.2]*.

**Day1's SaaS offering with Infor:** With the Infor Cloud environment, the customer will not need to purchase additional hardware. The applications are easily accessible through a modern browser.

### 1.22.2 Installation of new Infrastructure Responsibility Model [RFP 8.22.2]

---

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

In order to effectively procure, operate, and manage a cloud infrastructure in AWS, NASPO will require a certified partner who can help assume some of the obligations the "Customer/Partner Responsibility" model. Day1 understands that management of a cloud based environment requires a clear delineation of management and security responsibilities between the CSP and NASPO. Day1's review of the NASPO solicitation has allowed us to identify a number of requirements that are outside the scope of a traditional CSP and would require an additional level of support services from vendors such as Managed Service Provider (MSP) and Systems Integrator (SI) partner to deliver these capabilities. While a traditional CSP provides the ability to procure cloud infrastructure, there must be considerations for the management of that infrastructure.

AWS does not access customer data, and customers are given the choice as to how they store, manage and protect their data. Day1 believes that NASPO requires a cloud vendor to have fully developed managed service capabilities. Managed services capabilities help customers design, architect, build, migrate, and manage their data, workloads, and applications in the cloud. AWS's operating model clearly delineates the responsibility of controls between AWS and its customers.

The strengthening of NASPO's management and security posture includes identifying the boundaries of responsibility between AWS and NASPO. In order to do so, NASPO must have a service provider capable of supporting the Responsibilities Model as outlined by AWS. *Figure 49: MSP Responsibilities Model* below provides a high level overview of that Shared Responsibilities Model and provides insight into the areas where Day1's Managed Services can help to offset responsibilities that are defined by AWS.

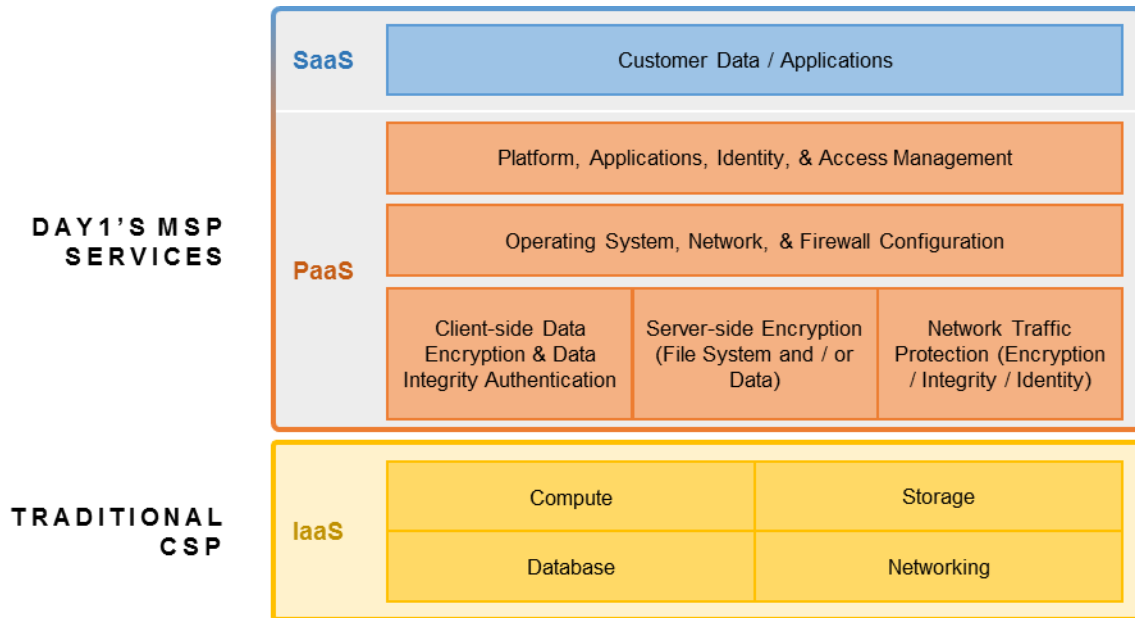


Figure 49: MSP Responsibilities Model

**Day1's SaaS offering with Infor:** Infor offers a true SaaS model, all inclusive of the infrastructure and software.

### 1.23 (E) Alignment of Cloud Computing Reference Architecture [RFP 8.23]

Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

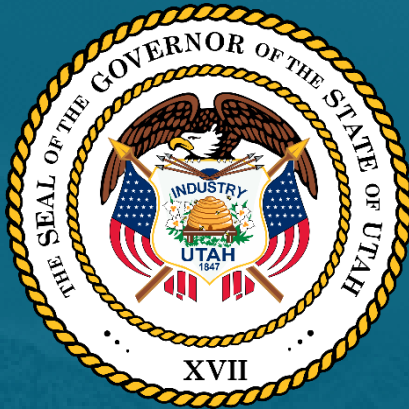
Under Section 1.1.2 NIST Characteristics [RFP 8.1.2] Day1 has provided NASPO with a highlight of our understanding of each NIST characteristic, in addition to an explanation of how our solution satisfies the NIST characteristics. Day1's offering of AWS is NIST compliant and directly compares to NIST Cloud Computing Reference Architecture as 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). AWS has leveraged federal security personnel with developing 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).

**Day1's SaaS offering with Infor:** Infor is a consumer of AWS's IaaS and PaaS services, and implement our SaaS solutions through AWS.

## 2.0 Appendix A

---

*This section has been redacted due to it being protected information. Day1 has existing NDA's in place with our clients allowing us to make references in proposals but not to provide it as a public reference. The disclosure of this information in a public forum, to include scope of work, architecture diagrams, system configuration, etc puts Day1 at risk of violating our NDA. . Please refer the Confidential, Protected or Proprietary Information Volume 7, Section 1.1. Appendix A (Technical Response ,Appendix A) for this information.*



State of Utah Division of Purchasing

# NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTION

CH16012

## ORGANIZATION PROFILE





# Contents

1.0	Organization and Staffing [RFP Section 7] .....	2
1.1	(ME) Contract Manager [RFP Section 7.1] .....	2
1.1.1	Contract Manger Contact Information [RFP Section 7.1.1] .....	2
1.1.2	Contract Manger Contact Information [RFP Section 7.1.2] .....	2
1.1.3	Contract Manager Roles and Responsibilities [RFP Section 7.1.3] .....	3
2.0	Resumes [RFP Section 7.1.2] .....	5

## 1.0 Organization and Staffing [RFP Section 7]

### 1.1 (ME) Contract Manager [RFP Section 7.1]

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

Day1 certifies that we currently have a Contract Administrator under the existing WSCA-NASPO contract and will continue to provide a Contract Administrator/Manager (Mr. Sean Wilson) as the single point of contact for management of the NASPO ValuePoint Master Agreement. Mr. Wilson is a manager in our PMO office and serves as the Contract Administrator for our current WSCA contract and where Day1 serves as one incumbent of only four providers. Mr. Wilson is a skilled contract manager with the proven ability to meet multiple deadlines, supervise large teams with varying backgrounds, and understand our client's mission and needs. A list of Mr. Wilson's qualifications and experiences over the last three years as a contract manager/administrator is as follows:

- Currently serves as Contract Administrator for Day1's WSCA Cloud Computing Contract – MA 265
- Mr. Wilson regularly interacts with NASPO and has an understanding of organization requirements to continue develop and drive business through the vehicle
- Mr. Wilson has first hand knowledge on the requirements and processes for onboarding new participating entities from guiding and overseeing participating addenda, engagement agreements, task orders, invoicing, etc.
- Mr. Wilson Previously served as Contract Administrator for Day1's US Census Public Cloud Indefinite Delivery/Indefinite Quantity (IDIQ) contract worth over \$24M
- Prior to working at Day1, Mr. Wilson served three years as a contract administrator for NITAAC CIO-SP3 Government Wide Acquisition Contracts with a contract ceiling of over \$20B

#### 1.1.1 Contract Manger Contact Information [RFP Section 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.*

The contact information for our Contract Administrator is as follows:

Name            Sean Wilson  
Phone            Cell 757.729.4352, Office 703.646.DAY1 ext. 414  
Email            sean@day1solutions.com  
Work Hours    8 AM – 6 PM Eastern

#### 1.1.2 Contract Manger Contact Information [RFP Section 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.*

Day1 is pleased to provide a copy our Contract Administrator/Manager's resume as included in Section 2 of this Organizational Profile volume. Additionally, an overview of Mr. Wilson's qualifications and experiences as a contract manager/administrator of contracts of similar size and scope has been provided:

- Mr. Wilson is a Project Management Institute (PMI) certified Project Management Professional (PMP) and is also certified in Amazon Web Services (AWS) to include AWS Certified Solutions Architect
- Mr. Wilson is a Shipley trained professional where he has fine-tuned his skills in business development, capture and proposal development processes
- As previously stated, Mr. Wilson currently serves as Contract Administrator for Day1's WSCA Cloud Computing Contract – MA 265
- Mr. Wilson was actively engaged in Day1's direct award of \$30M from the Maryland Department of Human Resources
- Mr. Wilson Previously served as Contract Administrator for Day1's US Census Public Cloud Indefinite Delivery/Indefinite Quantity (IDIQ) contract worth over \$24M
- Prior to working at Day1, Mr. Wilson served three years as a contract administrator for NITAAC CIO-SP3 Government Wide Acquisition Contracts with a contract ceiling of over \$20B

### 1.1.3 Contract Manager Roles and Responsibilities [RFP Section 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.*

Our Contract Administrator/Manager plays a vital role in ensuring Day1's success on the contract through meticulous management of the ongoing activities between Day1, NASPO, and participating entities. In order to provide Mr. Wilson with a high degree of autonomy, Day1 has provided him with complete authority over the operations and maintenance of this vehicle. At a high level, the roles and responsibilities required by Mr. Wilson as the Day1 Contract Administrator/Manager is as follows:

#### **Contract Administrator/Manager**

- Principal Point of Contact for NASPO
- Signature Authority
- Oversee contract/ participating addendum compliance within terms and conditions
- Lead NASPO Contract and Participating Entity Review Meetings
- Monitor/ control overall contract performance, including schedule and budget
- Negotiate and approve proposed purchase order cost estimates and schedules
- Assign each purchase order to State Account Teams
- Engage in escalated customer support/ issues when appropriate

Additionally, our contract administrator will work closely with our Usage Report Administrator to and help to oversee the following activities:

- Prepare and implement Project Management Plan, Quality Management Plan, and Quality Assurance Surveillance Plan (QASP)
- Implement Quality Audit with NASPO and Contract Administrator
- Provide Usage Reports to NASPO and Participating Entities
- Implement performance improvements to management and quality systems and processes
- Offer guidance on approach and personnel for program management services
- Engage in customer support when appropriate

## 2.0 Resumes [RFP Section 7.1.2]

### Sean Wilson

Contracts and Capture Manager

#### PROFILE

Skilled Contracts and Capture Management professional with the proven ability to meet multiple deadlines, supervise large teams with varying backgrounds, and understand the customer’s mission and needs. Certified Project Management Professional (PMP), AWS Certified Solutions Architect (CSA) and Shipley trained.

#### PROFESSIONAL EXPERIENCE

##### Day1 Solutions, Inc.

Principal Solutions Architect

August 2015 to Present

- Currently, Contract Manager for NASPO-WSCA (ValuePoint) Public Cloud Hosting Contract
- Principal Point of Contact and Signature Authority for WSCA
- Oversee participating and engagement addendum compliance within terms and conditions
- Work with VP of Delivery to plan and provide team resources
- Authorize SOW and purchase order negotiations
- Lead WSCA Contract and Participating Entity Review Meetings
- Enforce accountability
- Conduct Quality Audits
- Engage in escalated customer support/ issues when appropriate
- Contract Manager for Census Enterprise Solution Framework (ESF) For Cloud Computing Services
- Lead capture efforts on new and upcoming Task Orders
- Work with VP of Delivery to plan and provide team resources

#### PROFESSIONAL HIGHLIGHTS

##### EDUCATION

- BA, English, Virginia Tech

##### CERTIFICATIONS & TRAINING

- Project Management Professional (PMP)
- AWS Certified Solutions Architect (CSA) - Associate
- AWS Business Professional
- AWS Technical Professional

##### EXPERIENCE

- More than 5 years of project management experience in high paced environments
- Experienced Contracts Manager overseeing programs from contract inception to closeout
- Experienced in the full lifecycle of IT projects, from initial conception through design, prototyping, testing, implementation, training, and maintenance
- Expert in the guidance, governance and implementation of on-premise and cloud based IT technology and solutions to support Public Sector and commercial clients.

- Engage in escalated customer support/ issues when appropriate
- Ensure compliance with contract terms

## DMI

Contracts and Capture Manager  
September 2012 – July 2015

- Contracts Manager on our Task Order contract vehicles, CIO-SP3 and DOL BLS BPA, where DMI provides Information Technology services from mobility and software development to cloud and enterprise architecture solutions.
- Ensure compliance with contract terms on our major contract vehicles
- Principal Point of Contact for CIO-SP3 and DOL BLS
- Lead planning, documenting, and managing of capture project efforts, to include strategic wins at new agencies - NIH and DOJ
- Led strategic capture efforts for EPA business, including two highly visible mobility and cloud opportunities estimated at over \$100M in revenue
- Upon EAGLE II award, provided strategic research and analysis of the DHS mission and landscape and created a DHS “Smart Book” providing our team with a strategic roadmap to begin capture on new and existing DHS opportunities
- Provided capture and proposal support for strategic recompetes at DHS, HHS, and DOL
- Worked with account leads, executive leadership, and PM's to determine potential customer needs to fulfill the requirements of the opportunity
- Led information gathering and solution sessions to build a solution and ultimately a capture plan document
- Served as primary point of contact between the proposal and account lead teams
- Provided guidance to the Proposal Manager and sometimes act as Proposal Manager
- Participate in all major proposals reviews and lead my own reviews
- Prepared multi-million dollar winning proposals under tight deadlines, to include CNRSE, a strategic 15M dollar Navy project spanning 7 locations, including Cuba
- Reviewed and tailored content to comply with RFPs and convey strategic win themes
- Managed highly visible Government-wide OASIS IDIQ Capture and Proposal efforts and made sure we were compliant with contract terms

## Black Box Network Services

Proposal Writer  
December 2011 to September 2012

- Responsible for proposal writing and coordinating
- Coordinated input from multiple contributors and produced high-quality text in a short time frame

- Put in charge of managing and writing all Air Force Military Construction proposals, 3 per month
- Identified requirements and tracked compliance of proposal content
- Produced Training schedules and descriptions for Army proposals
- Edited documentation and presentations to ensure completeness, consistency, and conformity to prescribed formats
- Wrote/edited past performance summaries for proposals, including interviewing project managers to elicit data
- Helped build and maintain a library for Past Performance
- Assisted with business development activities; Included checking various BD sources such as GovWin, FedBizOpps, etc

## Prism Inc.

Technical Recruiter

December 2010 to December 2011

- Responsible for the recruitment process from identification to post hire procedures for positions such as Project Managers, Oracle/SQL DBA, Web Developers, etc.
- Broke into 4 new federal accounts (DHS and DoD) across a 6-month period by successfully recruiting and placing IT contractors within those clients.
- Considered the go-to recruiter for difficult to fill requirements within the DoD and DHS; Successfully filled TIBCO, Documentum, and Maximo positions which were all account breakers and required clearances
- Reformatted resumes and created submittals for candidates
- Organized all progress in Excel and Recruiting Database(Bullhorn)
- Interfaced between Business Developers, Clients, and Candidates

# Luis Benavides

CEO & Founder

Mr. Benavides is the CEO & Founder, and brings 17 years of successful sales and consulting experience to the Day1 team and will oversee this engagement. Mr. Benavides has a wide network of VAR, ISV, and SI relationship in the IT industry he has nurtured over the years. Mr. Benavides’s extensive ability to focus on skills will help drive individual work efforts, and keep the team motivated and on track for a timely completion.

## PROFILE

Accomplished sales and consulting professional who demonstrates an understanding of aligning opportunities with business goals and sales strategy. Has a wide network of VAR, ISV, and SI relationships built and nurtured over the years. Adept ability to focus on sales quarter objectives and develop/execute long-term plans. Values customer and partner relationships, and has spent the past 17 years building them as part of some of the most prestigious companies in the Country.

## PROFESSIONAL EXPERIENCE

### Day1 Solutions, Inc.

CEO & Founder

June 2012 to Present

- Founded Day1 Solutions in June of 2012. Oversaw the company growth in revenue from \$180K in 2012, to 122% growth in 2013, 1,525% growth in 2014, and projected 360% in 2015 & 100% in 2016. Started the company with own personal funds and attracted investors over time. Built what is considered the model Cloud Company focused on the customer needs for One Vendor, One Bill, As A Service.

### Amazon Web Services

Principal Sales Executive

April 2011 to June 2012

- Third employee hired by Teresa Carlson, VP of WWPS, to build the channel business unit. Set the strategy, resource plans, and goals for ISV, SI, and VAR partners of AWS, including program development with corporate counterparts from Terry Wise’s organization. Achieved over 50% of WWPS revenues based on partner revenue through my efforts in starting the channel/in-direct business model.

PROFESSIONAL HIGHLIGHTS
<b>EDUCATION</b> <ul style="list-style-type: none"> <li>• BS, Computer Science, Strayer University</li> </ul>
<b>CERTIFICATIONS &amp; TRAINING</b> <ul style="list-style-type: none"> <li>• AWS Business Professional</li> <li>• AWS Technical Professional</li> <li>• AWS TCO &amp; Cloud Economics</li> <li>• NetApp Accredited Sales Professional</li> <li>• Juniper Networks Sales Master</li> <li>• SA Security Sales &amp; Sales Engineer Associate in both Security Management &amp; Authentication Tracks</li> </ul>
<b>EXPERIENCE</b> <ul style="list-style-type: none"> <li>• Sales professional with 20 years of public sector sales, management, business development, market research and consulting experience.</li> <li>• Significant direct sales &amp; partner alliance experience for virtually all leading technology vendors and resellers serving the public sector.</li> <li>• Extensive knowledge in OEM, reseller and distribution channels.</li> <li>• Qualifications include: Revenue &amp; Profit Growth; Lead Generation &amp; Qualification; Opportunity Shaping; Channel Development &amp; Partner Management; Business Development; Customer Relations; Account Management Professional Services; Program &amp; Project Management.</li> </ul>



## NetApp

### Business Development Manager

June 2009 to April 2011

- Worked across all areas of business; from sales, marketing, executive leadership, corporate and global teams, services, channel. Fed, SLG, EDU, and Health verticals, interacting primarily with Sales Leaders and Sales Managers.
- Quota for All-Up Public Sector, driving growth from \$650M to \$800M, ranking #1 Storage Vendor to the Federal Government (doubling closest competitor EMC).
- Originally focused on Alliance partnership with Microsoft, but expanded to any industry partners that together could solve our customer's challenges and meet their goals. True entrepreneur model within an established company.
- Initially approached President to allow me the opportunity to create my own charter. My success influenced all of NetApp to designate two official new roles for Alliance field relationships, BDM and Business Solutions Architect.
- Changed from just driving incremental revenue to owning complete end-to-end solution GTM. Either from corporate to field, or created out of target market demand. Create-Package-Market-Sale-Results-Modify-Repeat
- Always selling sales teams on "Why this Partner solution will help their customers?" (revenue) or vice versa to Alliance and VAR partners. Developed VAR "Solution Champions" and GTM through SIs and TSPs for program capture.
- Briefed executives, met with customers, presented to large audiences, and active in social marketing.

### Microsoft Consulting System Engineer

October 2007 to May 2009

- Role at NetApp was that of a Microsoft Solutions Architect for the US Public Sector Sales team. This includes working with the FSI and Program Capture teams as well with the Office of the CTO.
- Mid Atlantic EBC Presenter for NetApp USPS and Commercial/Enterprise. Customer range from engineer, technical decision maker, C-level executives and VPs. High deal closure scores and feedback.
- Carried a quota for the "All-Up" number. Federal growth from \$350M to \$650M during my term.
- Responsible for training of SE staff, Territory Specialists, and Partners on NetApp's Microsoft Solutions.

## EMC

### Technical Architect

July 2002 to September 2007

- For Transportation Security Administration (TSA), my role on the EMC team was that of a Technical Architect focused on Microsoft Messaging and Collaboration. This included working with the Messaging System Implementation Team led by Unisys to deploy the prior "Microsoft AD/EX Redesign".
- Daily interaction with TSA stakeholders and decision makers across US Coast Guard and various DHS agencies.

- Worked with EMC DHS Sales team to identify business development opportunities for growth inside the account.
- Defined SOW and RFP program capture responses for other sales opportunities outside of billable contract.
- TSA contracted EMC for a “Microsoft AD/EX Redesign”, scaled from 100,000 users to all of DHS. This included designing TSA’s Intranet and Extranet Collaboration Document Management System (SP and LCS).
- For the Defense Finance and Account Services (DFAS), my role was that of a Technical Architect sub contracted by Booze Allen Hamilton. Our team designed a two site COOP/Disaster Recovery solution. Presented to BAH upper management and to the DFAS stakeholders on a regular basis.
- For DISA, I provided technical leadership as a Senior Engineer (sub-contracted by SRA International) to design and implement a Next Generation Collaboration portal for the Global Enterprise Services (GES) community based on Windows 2003 Active Directory, Sharepoint 2003 and Live Communications Server (LCS).
- Presented to CIO’s and Directors of various DoD commands on secure collaboration in the DoD enterprise.
- For SRA International implemented a Novel to Windows 2000 Active Directory migration. SRA contracted Internosis to present a case to implement a Windows 2000 enterprise solution. I was responsible for creating the pilot environment and technical documentation, then presented to SRA Internal IT TDMs.
- Assigned as a deployment Team Lead (sub-contracted by Telos) providing technical and management services for the Army Enterprise Infrastructure Transformation (AEIT) migration. Microsoft's largest Active Directory deployment up to that date (1.5M user environment).

## Standard Technology

### Senior Network Engineer

August 2001 to July 2002

- Contracted (sub to EDS) to the Department of the Navy Headquarters Network and Command Control Center at the Pentagon. Classified and Unclassified Network Supporting DoN HQ, MidA, and NMCI transition.
- Created engineering Action Plans, failure/trouble reports, and SOP’s; leveraging my technical writing skills.

## AmerInd

### Network Engineer

January 2000 to August 2001

- Responsible for administration of the Air Force and Army National Guard Bureau; supporting over 2,000 users, on the NOC Level III team for troubleshooting and overseeing daily operations of the Windows NT Enterprise.
- This role required interaction with Executives, Directors, and Officers. Commended numerous times for my professionalism and customer support.
- Involved with EDS re-bid for Air and Army support contract.

## Open Systems Sciences (OSS)

### **Assistant Supervisor of Technical Services**

August 1998 to December 1999

- OSS was a HP and Gateway VAR. As a Lead Engineer at OSS' Technical and Integration Facility, I managed a team building and configuring large customer orders (desktops and servers).
- Level I and II field service support for end-user contracts; i.e. SSA, Walter Reed Army Medical Hospital, Department of the Navy, and the US Coast Guard.

### **Systems Engineer**

May 1997 to July 1998

- Provided implementation engineering services of LAN systems "from the ground up" (cabling, rack mounting, testing, etc) for Military Sealift Command Atlantic.
- First IT Industry job that started as a part time role, and quickly became hired on staff.
- At OSS I developed an enduring methodology to troubleshooting; which has stayed with me throughout the years.

## Bob Vuong

Director of Consulting Practices

Mr. Bob Vuong has extensive experience with full project life-cycle implementations utilizing established and emerging technologies in various roles including program manager, solutions architect, systems integrator, systems engineer, and subject matter expert. Mr. Vuong has skills in managing and monitoring multiple million dollar programs to include maintaining schedules, budgets, and reports. As a Director of Consulting Services Mr. Vuong has been chartered in developing and standardizing consulting practices for federal customers within a fast-pace environment with assessing, designing, and implementing their cloud strategy and vision. Areas of support include, but are not limited to cloud architecture reviews, cloud migration, high-availability designs, security best practices, and pre-sales/capture support.

### PROFILE

An innovative and solutions-oriented senior-level Program Management and Information Technology professional contributing close to two decades of large-scale infrastructure experience working in all facets of IT, relationship, and technical project management. Expertise in IT life cycle and architecture, data resource management, and information technology infrastructures. Excelled in numerous high profile project advisor roles for a global corporation involving IT systems implementations. Proven leadership with customers, consistent quality in technical development of colleagues/subordinates, and a verifiable track record of successfully developing individuals and building and directing high-performance teams to maximize performance and proactively capitalize on opportunities that increase profit margins.

### PROFESSIONAL EXPERIENCE

#### Day1 Solutions, Inc.

Director of Consulting Practices

Time Frame

- Responsible for the development and maturity of federal pursuit, capture and business development efforts

### PROFESSIONAL HIGHLIGHTS

#### EDUCATION

- Over 17 years of experience directly related to architecture, installation, configuration and support of best-of-breed IT solutions and technologies
- Held multiple senior executive roles within highly aggressive IT organizations
- Experienced in the full lifecycle of IT projects, from initial conception through design, prototyping, testing, implementation, training, and maintenance
- Expert in the guidance, governance and implementation of on-premise and cloud based IT technology and solutions to support commercial and Public Sector clients
- Chartered with the development of multiple organizational verticals

#### CERTIFICATIONS & TRAINING

- AWS Business Professional
- AWS Technical Professional
- Project Management Professional (PMP)
- Microsoft Certified Professional (MCP)

#### CLEARANCE

- DoD Top Secret

- Develop standards and best practices in consulting services as it relates to federal, state and local government delivery
- Create practices around IT transformation practices and entire project lifecycle management
- Establish relationships between small, medium, and large system integrators
- Federal account management between civilian, DoD and intelligence community
- Assessed emerging technologies for corporate adoption
- Develop, pursue, and capture government contract vehicles
- Sourced, selected, and managed vendor relationships/ strategic partner initiatives
- Prepare, and present executive level presentations for the insertion of new organizational processes for proposal management
- Conduct and perform systems capacity planning, performance tuning, and monitoring as needed for external customers
- Define, set, and implemented architectural and engineering policies, procedures, and standards; aligned business needs with appropriate industry standards and trends

## Emagine IT

### Director of IT Infrastructure

#### Time Frame

- Led the maturity and continual development of IT Infrastructure capabilities, and consulting service offerings to include cloud, mobility, datacenter management/consolidation, operations and management, and IT service management
- Served as Program Manager on Emagine IT's largest program with over 50 FTE's providing IT Infrastructure Support, Governance, and Security Services the EIT Program Management Office (PMO) program at the Office of the Chief Information Officer (OCIO) at the National Resources Conservation Services (NRCS) for the US Department of Agriculture (USDA)
- Provided overall project management, through leadership and technical expertise to the EIT team on all OCIO initiatives through all phases of product life cycle development including requirements gathering, systems analysis, infrastructure architecture, and project implementation
- Supported corporate and backoffice activities to include business development and capture strategy development. Developed call plans to help grow work both horizontally and vertically within the USDA and NRCS
- Transformed project requirements into working architecture and translated business initiatives into technical solutions.
- Successfully grew work horizontally and by penetrating two additional USDA agencies and achieving three sole source awards
- Served as capture and proposal manager in Emagine IT's penetration into the Small Business Administration. Successfully won the Enterprise Architecture Support Services

- Developed capture strategy to procure additional contract vehicles and GWACs to include CIO-SP3 and Alliant Small Business

## Booz Allen Hamilton

### Lead Associate

#### Time Frame

- Project Manager and Infrastructure Team Lead for Booz Allen Hamilton's support of the Office of the Chief Information Officer (OCIO) at the Alcohol Tobacco Tax and Trade Bureau (TTB)
- Served as Lead for over 20 TTB IT Infrastructure team members consisting of Booz Allen employees and subcontractors
- Direct report to TTB's CIO and ACIO's with responsibilities such as program management and oversight, IT strategy development, developing and maintaining an IT budget, and shaping Enterprise Architecture
- Provided guidance and expertise to TTB CIO and ACIO's regarding relevant and emerging technologies such as desktop virtualization, thin clients, server virtualization, mobile computing, cloud computing, etc.
- Primary responsibilities to the Infrastructure Team include providing thought leadership and technical guidance to the Infrastructure team from requirements gathering to systems analysis, infrastructure architecture, and project implementation
- Highly involved with authoring and developing all IT Infrastructure related Statement Of Work (SOW), Performance Work Statements (PWS), and Request For Proposals (RFP)
- Established a service catalog and develop shared service offering for Infrastructure services within TTB.
- Served as the POC for all Infrastructure Shared Services between TTB and Community Development Financial Institutions (CDFI) IT services integration initiative
- Developed call plans and led market penetration efforts to bring Infrastructure Shared Services offerings to other departments within Treasury

## EMC's Microsoft Practice

### Senior Practice Consultant

#### Time Frame

- Provided expertise and consultation on Microsoft oriented products such as Microsoft Active Directory and Microsoft Exchange at The American Red Cross and Covance Pharmaceuticals
- Lead all joint architecture design sessions with Covance stakeholders regarding Microsoft Exchange and all messaging related technologies
- Advised Covance stakeholders on creating business requirements of the new messaging infrastructure that directly align with IT functionality and capabilities
- Lead effort for storage sizing of messaging services and assist with defining storage requirements for both Covance and The American Red Cross
- Assisted in the design of Covance's future messaging infrastructure consisting of over 30 centralized servers including technologies such as Microsoft Exchange 2007, Enterprise Vault 2007, BlackBerry Enterprise Server 4.1.5 (BES), and SQL 2005 all using Direct Attached Storage (DAS)

- Guided Red Cross management on defining business requirements, IT specifications, and end user needs related to the new Microsoft Exchange messaging environment and “One Infrastructure”
- Engaged in the writing and presenting RFCs (Request for Change), and RFPs (Request for Proposal) in the presence of Red Cross upper management and CCB (Change Control Board)
- Served as one of two primary Exchange experts to design a more centralized Exchange 2003 architecture utilizing fibre attached clustered servers, dedicated public servers, Bridgehead servers, etc., supporting over 40,000 users

## Northrop Grumman Information Technology

### Network Systems Engineer II

#### Time Frame

- Served as primary systems administrator for the Uniformed Services group and solely responsible for providing a stable and secure production and development environment
- Held responsible for configuring, deploying, and maintaining all racks, servers, and mission critical equipment for both production and development environments
- Held accountable for supporting all local and remote users by providing daily network support, and resolving connectivity issues with dial-up and VPN in addition to troubleshooting IT related problems
- Held responsible for all control access related activities within Uniformed Services such as creating Windows file shares, and assigning rights and permissions
- Performed all duties involved with integrating Uniformed Services’ domain into the corporate wide implementation of Active Directory

## Tony Witherspoon

Principal Solutions Architect

Mr. Tony Witherspoon has broad experiences with full project life-cycle implementations utilizing established and emerging technologies in various roles including solutions architect, software engineer, systems integrator, systems engineer, and project lead roles. Skills in managing and monitoring multiple project schedules, budgets, and reports. As a Principal Solutions Architect he supports commercial and federal customers within a fast-pace environment with assessing, designing, and implementing their cloud strategy and vision. Areas of support include, but are not limited to cloud architecture reviews, cloud migration, high-availability designs, security best practices, and pre-sales/capture support.

### PROFILE

A cloud solutions architect with various certifications (AWS Solutions Architect – Professional Level, ITILv3, Scrum, PMP) and the understanding that business objectives drive technology decisions. His diverse certifications and expertise range from project management, software development, systems architecture, cloud implementations, etc. Mr Witherspoon supports the design, architecture, and implementation of AWS based solutions for on-premise, hybrid and cloud platforms. Mr Witherspoon has over 16 years of technical engineering and consulting experience in the public/private sector both international and domestic and over six years supporting the Intelligence Community.

### PROFESSIONAL EXPERIENCE

#### Day1 Solutions, Inc.

Principal Solutions Architect

September 2012 to September 2013, April 2015 to Present

- Responsible for implementing and managing AWS cloud related research projects, proof-of-concepts, studies, and whitepaper deliverables both internally and customer related
- Provided technical training, leadership, and skills development for engineering staff
- Supported the creation of Day1's technical and business cloud service offerings
- Managed the development of offerings such as Amazon Web Services (AWS) Architecture Reviews, Security Best Practice Reviews, Cloud Strategy Workshops

### PROFESSIONAL HIGHLIGHTS

#### EDUCATION

- BS, Finance, Virginia Tech

#### CERTIFICATIONS & TRAINING

- AWS Certified Solutions Architect - Associate
- AWS Certified SysOps Administrator – Associate
- AWS Certified Solutions Architect – Professional
- AWS DevOps Engineer – Professional
- PMP Certified
- ITIL v3 Certified
- Certified Scrum Master
- Java (Sun Certified)
- Chef Fundamentals Training
- Chef Intermediate Training

#### EXPERIENCE

- 16+ years of IT experience related to architecture, configuration and support
- Experienced in the full lifecycle of IT projects, from design, prototyping, testing, implementation, training, and maintenance
- Expert in the guidance, governance and implementation of cloud based solutions to support commercial and Public Sector clients.



- Led customer engagements supporting their implementation of AWS services such as EC2, ELB, S3, EBS, VPC, Direct Connect, Glacier, and IAM in both public and hybrid cloud deployments
- Worked closely with Day1's CEO to help define, develop, and implement technology plans, solutions, and research and development efforts focused on leveraging cloud technologies to deliver business value
- Defined, set, and implemented architectural and engineering policies, procedures, and standards; aligned business needs with appropriate industry standards and trends
- Conducted and performed systems capacity planning, performance tuning, and monitoring
- Provided subject matter expertise in the response to public and private sector solicitations

## Booz Allen Hamilton

### Cloud Solutions Architect

April 2014 to April 2015

- Supported the adoption of public cloud infrastructure and technologies as part of the Booz Allen's Strategic Innovation Group (SIG)
- Provided cloud consulting, strategy, and architecture support across industries as well as supporting efforts for commercial, DoD and IC agencies
- Leveraged multiple AWS services in support of developing internal and customer proof of concepts (POCs) utilizing the Amazon cloud
- Designed the AWS architecture and supported the Chef components of a build management system leveraging the AWS cloud including Chef Server setup and Cookbook development
- Led the AWS architecture, design, and deployment activities for a cloud security proof of concept supporting a large energy client with a focus on defending and mitigating the insider threats
- Supported a multi-agency Joint Technical Taskforce (JTT) as an AWS SME supporting validating & mapping the NIST SP 800-53 rev. 3 controls to the services provided by the Commercial Cloud Services (C2S) implementation for IC ITE
- Identified and analyzed customer requirements and participated in responses to RFPs, RFQs, and RFIs with a primary focus on cloud and AWS solutions

## Leidos (formerly SAIC)

### Chief SW Systems Engineer

June 2013 to April 2014

- Led technical relationship and served as technical account manager for Amazon Web Services (AWS) relationship for Leidos.
- Led cloud research efforts in cloud management, cloud brokerage, and hybrid cloud deployments
- Implemented evaluation and proof of concept efforts of several cloud brokerage tools (CompatibleOne, ServiceNow, and others) to manage and deliver security as a service offerings across AWS and Rackspace
- Leveraged AWS services (EC2, ELB, S3, EBS, VPC, IAM, CloudFormation, etc.) and other tools (Eucalyptus, Cato, Git, Puppet, OpenVPN) across a hybrid cloud environment

- Identified solutions and best practices in cloud brokerage to manage cloud costs, usage monitoring, log analysis, auditing, compliance, key management, encryption, intrusion detection, and cloud migration
- Identified and analyzed customer requirements and participates in responses to RFPs, RFQs, and RFIs with a primary focus on cloud and AWS solutions

## SAIC

### Senior Solutions Architect

February 2008 to September 2012

- Part of a 3 person solutions architect team that is focused on shaping SAIC's cloud computing strategy. Directly responsible for multiple cloud research projects, proof-of-concepts, studies, and whitepapers
- Worked closely with SAIC Chief Technology Officers to help define, develop, and implement future technology plans, solutions, concepts, and research projects that can deliver mission value to customers
- Identified and analyzed customer requirements and participated in responses to RFPs, RFQs, and RFIs
- Led SAIC's efforts in developing a multi-tenant secure cloud reference architecture and framework
- Led and managed internal SAIC development effort to deliver a state government SaaS offering within the AWS cloud environment leveraging the AWS services (EC2, S3, VPC, RDS, ELB, and Route 53)
- Leveraged, deployed, and conducted vendor assessments and trade studies within Amazon EC2
- Chosen as one of the four SAIC representatives at the AWS Gov Cloud Summit II (October 2011)
- Attended several Amazon AWS seminars and training events to include: AWS 101, AWS 201, and AWS Architect training course that covers common AWS architecture patterns, AWS migration paths, and security best practices within AWS
- Assisted the USDA/FSA enterprise architecture in two Amazon EC2 proof-of-concept implementations (automated java build environment/hosted application)
- Co-wrote a 60+ page cloud computing survey and roadmap for USDA/FSA and personally responsible for conducting various trade study assessments on the current market leading IaaS and PaaS offerings
- Managed and directed Agency GCS project activities for several BlackBerry and Microsoft Exchange initiatives including the establishment of a Disaster Recovery capabilities for both systems
- Delivered key subject matter expertise to prepare and direct several projects through the Project Management Framework (PMF), governance boards, C&A process, and control gate milestones
- Generated and developed project documentation which included: System Design Specifications (SDS), System Requirements Documents (SRD), Deployment Plans, Configuration Management Plans (CMP), Risk Management Plans (RMP), System Security Plans (SSP), and a Requirements Traceability Matrix

## Lockheed Martin

### Staff Systems Engineer

June 2003 to February 2008

- Created and maintained system, configuration item, and design level requirements and their traceability from test to customer requirements utilizing Telelogic DOORS for a large 10 year program

- Generated, estimated, scheduled, and assigned project activities and the WBS for a multi-million dollar project in a large multi-contractor collaborative environment
- Supervised project activities, issue resolution, risk management, and internal communications across multiple groups and disciplines
- Managed and represented multiple projects at the contractor level bi-weekly reviews and technical exchange meetings tracking action items, issues, and risks to the project
- Followed the Project Management Framework (PMF) for developing project documentation and leading projects through all appropriate customer governance boards, which included guiding projects through the Agency Information Security approval process
- Managed, directed, and lead developer for J2EE development activities which include web development, DB administration, configuration management, system administration, and troubleshooting
- Prepared and conducted project reviews concerning the project schedule, milestones, risks, staffing, and budget presented monthly to the Advanced Technology Office (ATO) board members
- Served as point of contact for vendor and contractor relationships including contract negotiations, vendor management, and contract/license renewals

## John Hepner

Senior Sales Consultant – Public Sector

### PROFILE

Visionary enterprise sales leader of technology products into public and private sectors has earned awards representing customer satisfaction, top sales and partner acquisition. Trusted team mentor and coach develops high-performance global sales teams that exceed productivity and revenue targets. Innovative and adaptable territory developer exposes unexplored sales opportunities to boost profitability and client loyalty. Direct interpersonal skills establish credibility quickly and gain immediate respect and buy-in from stakeholders, vendors and members of cross-functional teams at all organizational levels.

### PROFESSIONAL EXPERIENCE

#### Day1 Solutions, Inc.

Senior Sales Consultant – Public Sector - State and Local Government, Education

September 2015 to Present

Responsible for helping clients leverage the WSCA/Naspo-ValuePoint contract for Public Cloud Hosting Services across the West and Central Regions of the U.S. Consulting with customers to help assess current business and IT needs and investigate new cloud adoption strategies to create efficiencies and reduce capital expenditures. Assist customers to accelerate cloud adoption and achieve a greater understanding of the cloud capabilities that help optimize their business. Drive sales of industry leading cloud based services by developing and executing against a comprehensive territory plan that includes; Reselling AWS Services, Consulting Services for Public Cloud Architecture and on-going Managed Services. Collaborate with AWS Public Sector Counterparts on strategies that facilitate adoption of AWS Services across named account territories.

Engaged with a Mid-Western State that is going through the process of adopting an Enterprise approach for public cloud procurement and deployment. The process requires engaging on multiple levels with resources within the customer, AWS and Day 1 Solutions to ensure success. Project is currently ongoing, with success in multiple workshops that include; Jumpstart project, Proof of Concept and Enterprise Cloud Governance.

#### Amazon Web Services

Public Sector Account Manager | State and Local Government, Education (Higher Ed & K-12)

April 2012 – July 2015

Drove sales of industry leading cloud based services by developing and executing against a comprehensive territory plan within Public Sector entities across the Central and West Regions and Canada; collaborated with AWS Partners

### PROFESSIONAL HIGHLIGHTS

#### EDUCATION

- BA, Business Administration / Marketing – University of Washington

#### CERTIFICATIONS & TRAINING

- Architecting on AWS – Amazon Web Services
- Private Cloud and Windows Azure Platform Solutions, Standards of Business Conduct, Diversity and Inclusion – Microsoft

#### TECHNICAL PROFICIENCIES

- SalesForce, Word, Excel, PowerPoint, Outlook, OneNote, InfoPath, Siebel CRM, Dynamics CRM

to extend reach and drive adoption across the territory. Called upon managed accounts and established relationships with C-level decision makers as well as software developers, IT Architects and demonstrated TCO of cloud bases services. Consulted with customers to identify use cases for priority adoption of AWS Services and implementation of best practices and leveraged AWS internal technical and business line resources to educate customers and drive solutions. Participated in association events and specific Public Sector conferences across the U.S. to generate new business and evangelize AWS Services.

- Engaged with large county in the Pacific Northwest to establish best practices around procurement of AWS Services and identify appropriate workloads to move to the cloud, leading to a savings of \$1 Million in the first year by archiving data in AWS.
- Created momentum with a key Southwest state and the CXO team to support their move to the Cloud by leveraging competitively bid contract vehicle and AWS Partners that led to massive savings and a clear path to move critical workloads to AWS Services.
- Worked with key law enforcement executive in Southern California to engage with AWS Compliance Team to provide expertise and guidance on CJIS – contribution to the publication of the AWS CJIS Compliance Whitepaper, August 3, 2015
- Identified innovative on-line school in Northwest as new AWS customer – developed Account Management plan that helped achieve their goal of shutting down their co-location facility and move their Data Center to AWS and achieve incredible savings and increase AWS Spend.

## Microsoft Corporation

### Public Sector Account Manager | State and Local Government

September 1991 to September 2011

### Public Sector Account Manager | State and Local Government

August 2006 to September 2011

Drove revenue by promoting services and solutions within city and county entities in the SE region; collaborated with field sales counterpart to manage 75 government accounts in four states. Called upon managed accounts and established relationships with C-level decision makers; overcame competitive threats by demonstrating product's ROI. Participated in association events and education events and formed relationships with senior decision makers.

- Nominated for several CPE awards for success in establishing the concept of trusted advisor among client accounts; regular meetings with clients' IT teams lifted technology competency levels
- Participated in events hosted by government IT professional associations across the territory to build relationships and show commitment to elevating IT knowledge; worked with association board members to plan quarterly member training events
- Conducted internal negotiations with BING Maps to attain \$15,000 in sponsorship funds to become a flagship sponsor for Georgia's Government Management Information Services (GMIS) international symposium; designed booth and secured keynote speaker for well-received event

### **Corporate Account Manager | US Headquarter Sales, Enterprise Partner Group**

January 2004 to August 2006

Managed two territories and 70 accounts encompassing the healthcare enterprise and automotive manufacturing segments; clients included Owens Corning, Sauder Woodworking and Volkswagen North America. Provided territory leadership by establishing territory plans, nurturing C-level relationships and orchestrating virtual team resources to drive customer and partner satisfaction, revenue and platform adoption. Articulated business value of products, services and solutions from technical and business solutions perspectives; customized message to address customer and industry needs.

- Selected from US sales team for Customer and Partner Experience Team Award in recognition of proactive customer service; drove customer confidence levels to become viewed as trusted advisors
- Exceeded \$2 million SQL Server quota by convincing customers to shift spend from Oracle
- Surpassed \$15 million revenue attainment goals by 122% of quota for three product groups

### **District Manager | US Headquarter Sales**

August 2000 to December 2003

Mentored team of up to eight corporate account managers working with enterprise and small and midmarket solutions and partners (SMS&P) in SE region; drove opportunity creation, management and velocity to exceed district business volume objectives. Recruited high-performing teams and filtered out low performers while minimizing business risk. Collaborated with field sales managers to ensure effective partner engagement and utilization strategy. Fostered open communication and partnership among HQ representatives and field counterparts. Contributed to strategic business planning; co-developed and executed territory plans.

- Overachieved district quota of \$108 million, attaining 135% of plan
- Won Enterprise Server MVP Award for driving recently acquired product Content Management Server opportunities in accord with the business marketing organization during a cross-sell campaign
- Stepped up to take on a special project involving a newly formed team of specialists focused on building Project and Visio business; facilitated team building for group dispersed across 18 nationwide districts and reported results to product groups to justify continued funding

### **Licensing Representative | Worldwide Licensing and Pricing**

October 1995 – July 2000

#### **Latin America**

July 1998 to July 2000

#### **North America**

October 1995 to July 1998

Negotiated licensing and pricing contracts with enterprise accounts, including banks, manufacturers and telecommunications companies. Collaborated with worldwide sales team as a licensing programs expert; shared agreement negotiation strategies designed to overcome customer objections, address competitive threats,

maximize revenue and boost customer satisfaction. Analyzed sales opportunities and competitive threats to develop creative and mutually favorable licensing strategies for enterprise customers; drafted enterprise agreement licensing proposals and amendments. Conducted presentations at executive briefings; communicated sales messages and enterprise agreement benefits to customers.

- Recognized for exceeding revenue and quota objectives while building fiscally sound agreements that creatively met the culturally and economically diverse business goals of client organizations
- Shared global Top Headquarters Contributor for Enterprise Agreements Award in recognition of creative deals with enterprise accounts such as ADP Dealer Services, MCI and Intel
- Traveled across Latin America to present two-day volume licensing trainings at multiple Microsoft subsidiaries; prepared more than 100 account representatives for enterprise agreement changes
- Created business momentum and suggested individual representatives for each Latin American country; leveraged relationships with local Microsoft offices to put plan in action

#### **Account Development Specialist | Microsoft Outbound Telesales**

March 1994 – September 1995

Presented products and conveyed strategies to corporate and solution provider account representatives. Managed accounts with key and emerging solution providers via face-to-face meetings and calls. Acted as partner account manager for PacWest District; presented product and partner recruitment seminars at the PWD Briefing Center.

- Selected for the District Performance Award for recruiting and managing 44 solution providers into the PacWest District via the Technology in Business Summit – Solutions Expo
- Identified and recruited 72 third party companies into the solution provider program; hosted vertical seminar and provided an overview presentation of BackOffice to 35 solution providers

#### **Account Management Specialist | Education Sales**

1993 – 1994

- Called upon managed higher education accounts to drive sales to campus resellers. Collaborated with internal departments to resolve questions on product availability and returns; provided sell-through information and determined pricing exceptions.
- Managed back to school sales at over 50 contracted campus resellers, garnering the highest district revenue out of 18 districts

# Tom Flynn

Director, Public Sector & Non Profit Sales

## PROFILE

Accomplished IT Sales professional with successful track record in information technology Business Development, Sales, Marketing and Consulting. Proven abilities in management, sales attainment, solution sales, bid and proposal endeavors and customer and partner relations. Possess a network of contacts in sales and marketing organizations throughout the information technology industry. Consistent results-oriented performer. Excellent communication skills and comfortable working with all layers and levels of staff within management, clients and business partners.

## PROFESSIONAL EXPERIENCE

### Day1 Solutions, Inc.

Director, Public Sector & Non Profit Sales

February 2015 to Present

- Lead Sales Executive responsible for inside and outside sales efforts, marketing and market research within Federal, State & Local, Higher Education and Nonprofit segments. Direct all customer delivery activities to ensure customer satisfaction
- Created various Systems Integrator & VAR teaming relationships with different revenue generating partners
- Lead and participated in various contract capture pursuits at AFGE, MCC, DOC, DHS, NASPO as well as numerous states throughout the country
- Manage sales team, coordinate capture pursuits and plan IT service engagements with VP, Services & Programs.
- Individual contributor as well as manager. Generated \$3M+ in Cloud IT related sales within various clients while mentoring and leading sales team.

### IT Sales Expert

Independent Consultant

February 2013 to February 2015

## PROFESSIONAL HIGHLIGHTS

### EDUCATION

- MS, Education
- BA, History

### CERTIFICATIONS & TRAINING

- AWS Business Professional
- AWS Technical Professional
- AWS TCO & Cloud Economics
- NetApp Accredited Sales Professional
- Juniper Networks Sales Master
- RSA Security Sales & Sales Engineer Associate in both Security Management & Authentication Tracks

### EXPERIENCE

- Sales professional with 20 years of public sector sales, management, business development, market research and consulting experience.
- Significant direct sales & partner alliance experience for virtually all leading technology vendors and resellers serving the public sector.
- Extensive knowledge in OEM, reseller and distribution channels.
- Qualifications include: Revenue & Profit Growth; Lead Generation & Qualification; Opportunity Shaping; Channel Development & Partner Management; Business Development; Customer Relations; Account Management Professional Services; Program & Project Management.



- Senior consultant and strategic advisor for companies and individuals reselling information technology to the Public and Commercial sectors.
- Advisory services include market research, competitive analysis, channels, sales strategy and solution sales, bid and proposal support and other ancillary services.
- Mentor and support clients in all aspects of the sales life-cycle with emphasis on the Public Sector vertical.

## Copper River

### Sales Representative

April 2006 to November 2012

- Responsible for inside and outside sales efforts within numerous Federal agencies, System Integrators and Prime Contractors as well as other IT VARs.
- Created numerous OEM reseller agreements and teaming relationships with different revenue generating partners.
- Lead and participated in various contract capture pursuits at USDA, DOC, NASA, USGS, DOE and other agencies.
- Generated \$2.5M+ in sales and \$300K+ in GP. Mentored sales team that generated over \$50M+ in sales in 2013. Contributed significantly to other revenue and profit attainment during tenure.

## Four Points Technology LLC

### Vice President

April 2006 to November 2012

#### Vice President, Sales (4/12 to 11/12)

- Responsible for P&L and staff of nine people (inside, outside and sales support).
- Generated over \$30M in sales. Managed a team that generated \$60M+ in sales and over \$4.6M in GP in 2012. Secured a new 3 year DoD Tri-care client contract worth \$6.3M annually.

#### Executive Director (4/06 to 4/12)

- Built and maintained manufacturer and integrator partnerships for a Small Business VAR/Integrator.
- Developed new business from market research, inside sales, outside sales and proposal writing activities.
- Responsible for P&L and staff of five people (inside, outside and sales support).
- Generated and managed approximately \$140M in sales and approximately \$9.7M in GP over period.
- Lead capture efforts for multiple contracts, Software Enterprise Agreements, Indefinite Delivery/Indefinite Quantity (ID/IQs) and Blanket Purchase Agreements (BPAs) at DOE, NASA, Labor, VA, USPTO, Treasury and multiple other Departments as well as with many major and mid-tier System Integrator Primes & Subcontractors such as Lockheed Martin, Northrop Grumman, General Dynamics, CSC, IBM, URS, SRA.
- Secured dozens of profitable new partnerships in networking, security, storage, and other segments.

## Apptis Inc.

### Executive Director, Partners & Programs

July 2000 to April 2006

**Executive Director, Partners & Programs (06/03 to 04/06)**

- Managed staff of six dedicated to qualifying, selecting and maintaining corporate partnerships for \$700M VAR/Systems Integrator.
- Led partner related business development and marketing functions.
- Drove corporate sales growth through increasing partner business and profitability via new alliances, markets and vendor soft dollar programs.
- Co-responsible for product bid and proposal efforts.
- Merged profit/loss center with another team and held annual quota exceeding \$330M in sales at over \$34M in gross margin for 2006.
- Managed own P&L center with annual quota of \$107M at \$10.2M gross margin in 2005. Net contribution to firm exceeded \$12.6M at over 120% of quota in 2005.
- Grew team from one to six employees. Ran P&L center with soft dollar quota of \$1.7M in 2004 achieving 105% of quota.
- Played integral role on Bid/Proposal team by performing market research, securing teaming agreements, negotiating pricing and supporting full bid life cycle. 90%+ success rate in major program bids supported. Contract wins included Army NETCOM BPA and NETCOM ESTA Security BPA, Army ADMC-2 BPA, NIH ECS III GWAC, Homeland Security BPA, IRS TCV BPA, Military Health TIMPO EUD BPA and others.
- Increased corporate sales pipeline by building alliances in strategic areas such as storage, IP telephony, wired/wireless networking, security and internet technologies across different verticals such as Federal, State and Local government, Education, Healthcare and Commercial markets.

**Director, Vendor Relations, Program Management Division (07/00 to 06/03)**

- Managed network of distributors, manufacturers and other partners involved in selling technology solutions to public and private sector customers for a Systems Integrator growing from \$130M to over \$300M in annual sales.
- Responsibilities included existing and prospective vendor partnerships, business development, bid and proposal, corporate marketing, contract coordination, staff and partner training.
- Created company's first Partner Program encompassing sales incentives (SPIF), Market Development Funds (MDF) and rebate programs. Generated \$1.8M in profitability and funded new marketing efforts.
- 90% success rate in major program capture supported. Contract wins included Army ADMC-1 BPA, US Customs BPA, US Forest Service BPA, BOP VTC BPA, US Courts BPA, VA PCHS-2 ID/IQ and others.
- Supported daily sales operations for teams comprised of Sales Managers, Program Managers, Account Executives and Inside Sales staff as well as all contracts including: GSA Schedule, Indefinite Delivery/Indefinite Quantity (ID/IQ) contracts and Blanket Purchase Agreements (BPAs).

## Federal Sources Inc. (FSI)

### Sale Director

February 1996 to July 2000

#### Sales Director, Internet Service Division (08/99-07/00)

- Managed and grew sales efforts for \$10M+ company.
- Co-responsible for \$1.3M budget, management of nine employees, corporate marketing, strategic alliances and new product launches.
- Grew product sales by 20% while reducing group costs 16%.
- Maintained 75% customer renewal rate - best in company history.

#### Senior Account Executive, Internet Service Division (08/98-08/99)

- Lead account executive and new business contributor for privately held firm sold to PRIMEDIA Inc.
- Exceeded group revenue goals by meeting individual quota and assisting team members in lead identification, proposal development and conducting client presentations.
- Developed and oversaw largest sales territory encompassing systems integration and service companies.
- Trained new staff and received various individual and group sales awards.
- Generated over \$2.4M in sales - 150% of quota.
- Negotiated 3 largest product contracts and 4 largest joint consulting/product agreements in firm history.
- Closed an average of 8 new customers per month.
- #1 Sales Executive of the month eleven times.

#### Sales Representative, Sales and Marketing Division (08/97-08/98)

- Generated new business from technology companies via telesales and web-based techniques.
- Created and maintained prospect process and sales forecasts.
- Provided product quality control, client support and technical assistance.
- Trained prospects and clients how to utilize FSI's Internet services to enhance their business development efforts.
- Exceeded quota by closing sales totaling more than \$1.1M.
- Assisted in creation of new business development model implemented by company that resulted in enlistment of approximately 75 new customers - 25% growth.

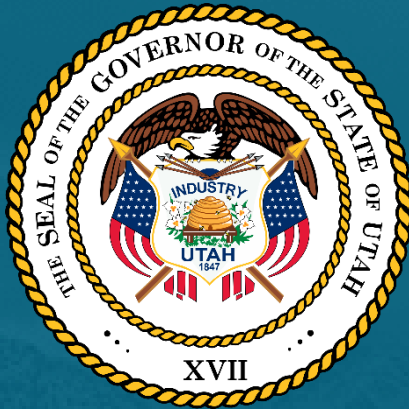
#### Federal Contract Analyst, Federal Division (02/97-08/97)

- Established relationships with numerous federal officials including CIOs, program and contract officers.
- Amassed and synthesized thousands of task orders for new IDIQ Tracking Service.
- Co-created newly released service's marketing collateral, press release and corporate presentation.

- Created new service ahead of schedule and under budget. Service purchased by 85% of client base.

**State and Local Research Analyst, State and Local Division (02/96-02/97)**

- Identified and tracked hundreds of technology projects and procurements at state and local level.
- Found and preserved government contacts.
- Qualified business opportunities that were successfully marketed to by System Integrators, IT VARs, Manufacturers (OEM), Consulting firms etc.
- Engaged in market and trend analysis to assist clients in prioritizing sales and marketing resources.
- Completed projects for state, local and vendor clients.
- Synthesized contract information and data for publication in national magazines.
- Top analyst in procurement opportunity identification and update cycle.
- Designed and implemented vertical and horizontal market studies successfully sold by consulting staff.



State of Utah Division of Purchasing

# NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTION

CH16012

## BUSINESS PROFILE



# Contents

1.0	Business Information [RFP Section 6]	2
1.1	(M)(E) Business Profile	2
1.2	(M)(E) Scope of Experience	8
1.3	(M) Financials	15
1.4	(E) General Information	17
1.4.1	Pertinent General Information	17
1.4.2	Auditing Capabilities	22
1.5	(E) Billing and Pricing Practices	22
1.5.1	Billing and Pricing Practices	22
1.5.2	Typical Cost Impacts	23
1.5.3	NIST Compliance	24
1.6	(E) Scope and Variety of Cloud Solutions	25
1.7	(E) Best Practices	27

## 1.0 Business Information [RFP Section 6]

### 1.1 (M)(E) 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.*

Day1 Solutions, Inc., (Day1) appreciates the opportunity to partner with the state of Utah and is pleased to provide our response to NASPO ValuePoint's Master Agreement for Cloud Solutions. Day1 looks forward to continuing our services as an incumbent cloud solutions partner through the NASPO ValuePoint. Day1 offers a purpose built cloud one stop shop for complete and innovative solutions to satisfy our customers' business requirements, reducing our customers' risk and expense. Day1 Solutions was established in Virginia in 2012 by our Founder and CEO, Mr. Luis Benavides. Mr. Benavides started his career supporting public service at the Military Sealift Command and also at the Pentagon as a contractor for the US Department of Navy Headquarters (DONHQ) supporting the National Capitol Region (NCR). As one of the first executives at Amazon Web Services (AWS) Mr. Benavides' vision was to develop an end-to-end cloud company that truly understood our customers mission. As our slogan states below, we have a mission centric approach to IT transformation, it is our belief that cloud is an opportunity for change.

### BECAUSE IT'S MORE THAN CLOUD®

...it's about saving lives, educating our youth, protecting our land, and disrupting the status quo. It's not about servers. It's not about storage. It's more than IT. It's about overcoming business challenges to achieve your mission and goals with speed & agility from **Day1**.

Day1 understands that as NASPO was purpose built (like many public service organizations) to solve the evolving need of public agencies to procure and implement cloud technology, and solutions like Geospatial Information Systems (GIS). Similar to NASPO, Day1 was also purpose-built with an evolved business model, and value-proposition to meet the needs of our cloud clients. Our approach is to surround a mission to be a comprehensive end-to-end cloud solutions provider (CSP) focused on AWS solutions, capable of combining the elements of a Value Added Reseller (VAR), Systems Integrator (SI), and Managed Service Provider (MSP).

- **Value Added Reseller (VAR):** As a Channel Reseller Partner, Day1 Solutions can provide direct access to the expansive catalog of services within AWS. Additionally, our extensive experience and partner level as a reseller provides state entities with an organization adept to the complexities of vendor management with AWS.
- **Systems Integrator (SI):** Our competencies as an Advanced Consulting Partner assure that Day1 will provide high-level consulting, architecture, design, engineering and other delivery related professional services.



































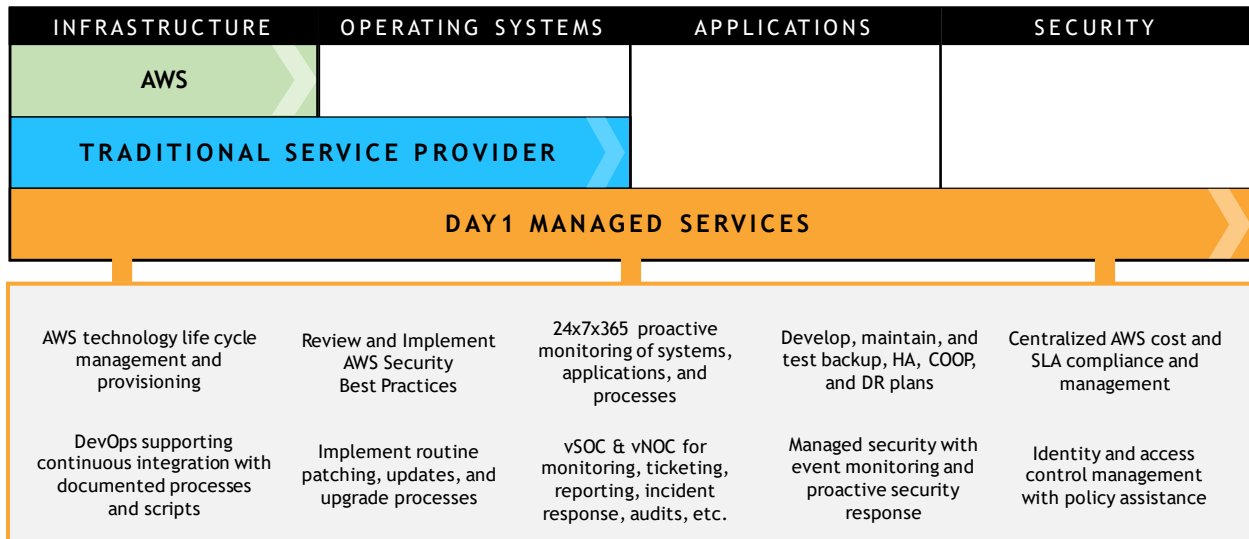


Figure 8: Depth and Breadth of Professional Services

AWS is the leader in Cloud technology and considered the defacto standard by Gartner when referring to cloud services and solutions. Below in *Figure 8: AWS Services and Descriptions* is a high level description of the AWS cloud platform categories that Day1 will bring immediately to the contract.

<b>DEPLOYMENT &amp; MANAGEMENT</b>		<b>SECURITY &amp; ADMINISTRATION</b>	
Services to help with management of credentials for access to AWS services, to monitor NASPO customer applications, to create and update stacks of AWS resource, deploy applications, use hardware security modules (HSMs) and log AWS API activity.		Services to help facilitate the security and administration of NASPO customer resources deployed in the AWS cloud. Implement controls to ensure an optimized shared security model.	
<b>APPLICATION</b>		<b>MOBILE SERVICES</b>	
A variety of managed services to use with organizational applications including services that provide application streaming, queuing, push notification, email delivery, and transcoding.		Unique services that facilitate and enable the development of mobile centric applications. Deploy, analyze, and test across multiple platforms.	
<b>DATABASE</b>	<b>ANALYTICS</b>	<b>ENTERPRISE APPLICATIONS</b>	
Fully managed relational and NoSQL database service, in-memory caching as a service and petabyte-scale data-warehouse service.	Cloud based analytics services to process and analyze any volume of data, whether it by managed Hadoop clusters, real-time streaming data, petabyte scale data warehousing, or orchestration.	A wide variety of enterprise level applications that provide NASPO customer with office automation capabilities.	
<b>NETWORKING</b>	<b>COMPUTE</b>	<b>STORAGE</b>	
A full range of networking services including logically isolated networks, private network connection to the AWS cloud, and highly available and saleable DNS service and deliver content to end users.	A wide selection of compute instances which can scale up and down automatically to meet the needs of NASPO customer applications, a managed load balancing service as well as fully managed desktops in the cloud.	Low-cost data storage with high durability and availability. AWS offers storage choices for backup, archiving, and disaster recovery, as well as block, file, and object storage.	
<b>AWS GLOBAL INFRASTRUCTURE</b>			

Figure 9: AWS Services and Descriptions

Being a Strategic Partner and reseller with AWS we also offer a comprehensive catalog of products that are used to provide the services mentioned in Figure 8 above. Day1 will offer State, local and educational entities with direct access to these products and services without the complications of billing, transfer of services, and delay in purchasing or obtaining these services through a separate reseller. A list of specific AWS technologies, and products can be found in *Figure 9: AWS Specific Technologies and Services* below. This provides an exhaustive list of AWS products and shows the depth and breadth of solutions our staff is capable of providing. Additionally, as an authorized AWS Marketplace Consulting Partner, Day1 can provide access to an extensive list of AWS Marketplace offerings. Key elements and highlights of these offerings include:

- AWS Marketplace offers more than 2,300 software products in 35 categories that customers can launch on AWS with one click.
- For software companies interested in making their products available to AWS customers, AWS Marketplace provides a method to develop PaaS and SaaS products.
- Customers run over 143 million hours a month of Amazon EC2 for AWS Marketplace products.






















































MANAGEMENT TOOLS	SECURITY & IDENTITY	DEVELOPER TOOLS	
 CloudWatch  CloudFormation  CloudTrail  Config  OpsWorks  Service Catalog  Trusted Advisor	 Identity & Access Management  Directory Service  Malicious Web Traffic (WAF)  Certificate Manager	 CodeCommit  CodeDeploy  CodePipeline	
APPLICATION SERVICES		MOBILE SERVICES	
 API Gateway  AppStream  CloudSearch	 Elastic Transcoder  Simple Email Service (SES)  Simple Queue Service (SQS)  Simple Workflow Service (SWF)	 Mobile Hub  Cognito  Device Farm  Mobile Analytics	 Simple Notification Service (SNS)
DATABASE	ANALYTICS	ENTERPRISE APPLICATIONS	
 Relational Database Service (RDS)  DynamoDB  ElastiCache  Redshift  Database Migration Service	 Managed Hadoop Framework (EMR)  Data Pipeline  Elasticsearch Service  Kinesis  Machine Learning	 WorkSpaces  WorkDocs  WorkMail	
NETWORK	COMPUTE	STORAGE	
 Virtual Private Cloud (VPC)  Direct Connect  Route 53	 Elastic Cloud Compute (EC2)  EC2 Container Service  Elastic Beanstalk  Lambda	 Simple Storage Service (S3)  CloudFront  Glacier  Import/Export Snowball  Storage Gateway	

Figure 10: AWS Specific Technologies and Services

Day1 is ready to make AWS Free Tier available to NASPO purchasing entities as a way to test AWS products and services prior to purchase. The AWS Free Tier can be leveraged by NASPO customers for a 12 Month Introductory Period and is only available to new AWS customers, and is only available for 12 months following initial AWS sign-up date. Day1 has guided new customers through the use of AWS Free Tier as a precursor to purchasing AWS services. Often, Day1 customers find AWS Free Tier has a handy tool to understand how products will be integrated into their environment and as a proof of concept prior to purchase. A full list of products and services that can be at <https://aws.amazon.com/free>.

Through our teaming partner, Infor, Day1 can offer NASPO Purchasing Entities the benefits of a global company with local presence and experience. Infor is changing will help to evolve NASPO's expectations from an enterprise software provider by delivering, through acquisition and innovation, proven business-specific solutions with experience built in. They show depth and breadth of industry experience to include:

- 19 of the 20 largest aerospace companies
- 12 of the 13 largest high tech companies
- 10 of the top 10 pharmaceutical companies
- 84 of the top 100 automotive suppliers
- 31 of the top 50 industrial distributors
- 6 of the top 10 brewers
- 8 of the top 10 U.S. integrated delivery networks
- 21 of the top 25 largest US health delivery networks
- 16 of the 20 largest US cities
- 19 of the 20 largest US states
- Over 1,200 state and local government agencies
- Over 3,000 financial services companies

Infor offers a complete array of products to manage key elements of business operations to include front office, back office, and supply chain operations. Infor can help to guide NASPO in redefining roles and responsibility to ensure that IT systems are accurately integrated into all segments of business to include:

- Enterprise Resource Planning
- Regulation, Permitting, and Enforcement
- Public Sector Asset Management
- Customer Information System (CIS) Billing
- Customer Relationship Management
- EnRoute Police and Emergency Dispatch
- Libraries and Information Centers
- Hospitality/Government Lodging
- Governance, Risk and Compliance (GRC)

- Construction Management/Property Management
- Public Sector Healthcare

#### 1.4.2 Auditing Capabilities

---

*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.*

Day1's use of AWS allows us to provide NASPO with a cloud infrastructure that has been designed and is managed in alignment with multiple regulations, standards, and best practices to include: 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). Additionally, Day1 has the ability to support auditing and reporting requirements of NASPO to be consistent with SAS 70, SSAE 16, or greater.

### 1.5 (E) Billing and Pricing Practices

---

#### 1.5.1 Billing and Pricing Practices

---

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

Day1 provides direct access to the AWS account billing and cost management portal. Our clients have the ability to have direct access to their billing content. This information can be ingested into many billing/reporting engines such as SAP and Oracle. This level of fidelity provides our clients with the ability to support charge-backs to the agencies. Due to the nature of the AWS billing structure, billing information such as hourly breakdown by resource or tagging is available if requested via an external platform.

The AWS Management Console provides the ability to manage all services and accounts. Day1 provides the ability to establish Consolidated Billing for multiple accounts. Day1 provides detailed billing reports and access to live usage reports to our clients so they have continual insight into their spending and usage trends. If needed for their use cases, Day1 will provision a client with more than one AWS account and can provide bills for those accounts jointly or independently. The pay-as-you-go model is key benefit of cloud computing, and we are pleased to be able to offer this benefit to our clients; Day1 has often provided infrastructure and consulting services as Time & Material, meaning the client pays only for what they actually use. This makes it easier to budget for possible future growth without worry of losing your investment should that growth not occur as predicted.

Day1 encourages and assists clients in making full use of AWS services and growth capabilities. Day1 does not limit or throttle client consumption of cloud resources, and, unlike many IT consultants, we allow our clients full and administrative access over their cloud resources. We do work with our clients to create usage and billing alerts for monitoring of consumption and cost. For those scenarios where multiple cloud platforms may be used, Day1 will work with you to select the appropriate third-party software for managing account billing across multiple cloud providers. Examples of third-party software solutions that might be used for these purposes include CloudCheckr and Orbitera. However, a number of other products and solutions exist that may be considered.

As an Authorized Government Partner, Day1 will receive all cost from AWS as part of our consolidated billing model. Once ingested into our accounting system we bill each of our clients directly based on the usage and consumption,

as well as any potential other fees that may be associated with the AWS account and services. With Day1 we have the ability to provision multiple accounts that would allow you to track cost by department. With AWS tagging, we have the ability to tag AWS services by department (unique ID) within an individual account, thus providing the end-customer with a single invoice that provides to do chargeback to the specific departments. Our team is well versed in AWS billing and both models outlined above. Our typical process is to work with the end-customer/s to identify the best practices that meet their unique business needs.

Under our agreements with AWS as an Authorized Government Partner and Reseller, Day1 will provide the provisioning and administration of the AWS account(s) to include AWS payment handling as well as the maintenance of top-level root account credentials. Accounts are secured using industry best practices including:

- Hardware multi factor authentication on root credentials
- Strong password requirements and password rotation for top-level credentials
- Root access keys are not generated
- Optional Security Challenge Questions enabled

Day1 will be the listed point of contact for the account, however AWS operations and security notifications regarding the account will be provided direct to the clients appointed administrator.

Day1 will provide a monthly invoice/s based on AWS usage, support and professional services if applicable. In an effort to continually provide our customers with a simple process of procuring cloud/IT services; we have taken steps to reduce the complexity by offering a percentage discount off MSRP for all Amazon Web Services (AWS) services and products authorized under our APN (Approved Partner Network) agreements. Also, as monthly price reductions are implemented by AWS, we immediately pass on those savings to our end-clients.

### 1.5.2 Typical Cost Impacts

---

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

As part any organization's journey to the cloud, there are considerations for costs outside of purchasing of the cloud commodity. As part of the process of instituting cloud-based services and solutions, organizations must to account for how the cloud eco-system will integrate with their existing on-premise IT platforms and business functions. Day1 asserts that the cost impacts listed below are considerations that all organizations must understand prior to the implementation of any cloud solution including those proposed by Day1:

- Workforce Transformation – Skill set alignment with cloud technology (Training)
- Billing & Cost Management – Virtual machine sprawl and quick provisioning may increase the number of servers deployed
- 3rd party licensing/migration tools – Migration of existing environments may require automated tools
- On-premise cost considerations (space, hardware, software, network, overhead cost) – Hybrid cloud solutions often require on-premise components
- Application Disposition (Lift & Shift, Refactor, Replatform) – Applications may have developmental costs if they are to be maximized for the cloud

- Governance & Security – New governing and security controls must be implemented to take advantage of the agility of the cloud to provision quicker to more places
- Operation Model – Typical system operations make way for new more forward thinking methodologies such as DevOps and require training and new tools
- Continuous Delivery/Continuous Integration – New delivery and processes require training and tools

### 1.5.3 NIST Compliance

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

Day1 understands the need for NASPO and all purchasing entities to have the ability to obtain cloud based solutions that meet NIST essential characteristics as it provides an industry accepted baseline for cloud based services. For the following sections below, Day1 has provided NASPO with a highlight of our understanding of each NIST characteristic, in addition to an explanation of how our solution satisfies the NIST characteristics. Day1's offering of AWS is NIST compliant as validated by two Agency Authority to Operate (ATO) 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). AWS has leveraged federal security personnel with developing 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).

**On-Demand Self Service:** NIST characterizes On-Demand Self-Service as the ability for consumers to unilaterally and automatically provision computing capabilities to include server time and network storage without manual intervention for each service. Day1 understands that self-service of IT resources is a compelling reason to leverage the cloud as it allows organizations to quickly provision IT resources without creating further deployment delays as characterized by an exhaustive procurement cycle. **How Day1's Cloud Solutions Satisfies NIST On-Demand Self Service Characteristics:** Day1 asserts that Amazon Web Services, Inc. (AWS) provides NASPO with the ability to meet these requirements as AWS provides consumers of all sizes with on-demand access to a wide range of cloud infrastructure services. An entire catalog of AWS On-Demand Self Service solutions can be found in the Day1 Technical Response.

**Broad Network Access:** NIST characteristics of Broad Network Access require that services are available over a network and accessed through standard mechanisms that encourage the use of heterogeneous platforms. Day1 understands that this independence from geography and deployment of services that are easily network accessible provides NASPO purchasing entities with great flexibility in deploying, connecting, and accessing IT resources. **How Day1's Cloud Solutions Satisfies NIST Broad Network Access Characteristics:** Day1 affirms that AWS complies with these characteristics as they provide a simple way to access servers, storage, databases, and a broad set of application services over the Internet through the AWS Management Console which will provide NASPO with the ability to provision services needed by each purchasing entity via a web application, mobile client, command line access through Secure Shell (SSH) or programmatically through published and well documented Application Program Interfaces (APIs).

**Resource Pooling:** The main NIST characteristics of Resources Pooling require that "the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand". Day1 understands the significance of resource pooling to NASPO purchasing entities as it ensures greater efficiency in IT services and provides for

economies of scale in pricing. **How Day1's Cloud Solutions Satisfies NIST Resource Pooling Characteristics:** Day1 is highly experienced in developing and architecting diverse cloud models and can provide NASPO customers with the ability to implement cloud models that provide resource pooling abilities based on the requirements of the customer. Leveraging AWS we can provide NASPO with a virtualized, multi-tenant environment that can be used by NASPO purchasing entities to support multiple cloud deployment models with specific resource pooling requirements that meet Public, Community, Hybrid, and Private requirements.

**Rapid Elasticity:** The NIST requirements for Rapid Elasticity state that resources should be provisioned and released elastically and may also require for automated scalability to meet rapid outward and inward demands. Day1 understands that the majority of cloud adopters seek the rapid elasticity afforded through the cloud as it allows organizations to quickly scale up (or down) resources based on demand. **How Day1's Cloud Solutions Satisfies NIST Rapid Elasticity Characteristics:** AWS provides a massive global cloud infrastructure that allows for quick innovation, experimentation, and iteration of services through elasticity in services and capabilities.

**Measured Services:** NIST requires that cloud systems allow for resource control and optimization through metering capabilities similar to a pay-per-use or charge-per-use basis. Day1 understands the importance of measured services to adequately forecast spend and allow for purchasing entities to control use of IT resources. Day1 will utilize AWS automated monitoring systems to provide a high level of service performance and availability. **How Day1's Cloud Solutions Satisfies NIST Measured Services Characteristics:** Day1 will leverage proactive monitoring 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 to ensure personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

## 1.6 (E) 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.*

Core components of AWS cloud infrastructure services include compute, storage and content delivery, network and database services. These core services provide the foundation for our existing ValuePoint clients while enabling a rich platform of services, such as analytics, enterprise applications, mobile services and Internet of things (IoT). Day1 is a strategic partner with AWS providing a host of solutions and services. As a reseller of AWS we offer our clients the ability to deploy all AWS developed IaaS, PaaS, and SaaS services as seen in *Figure 8: AWS Specific Technologies and Services*.

In conjunction with AWS core infrastructure services we offer the AWS Marketplace, which allows Day1 to provide our clients with reliable products and SaaS based solutions that integrate with their existing cloud based infrastructure. Under our existing participating addendums (PA) we offer our clients access to these services and solutions. These services and products can be consumed direct and deployed through AWS Identity and Access Management (IAM) console or via an integrated platform (AWS service catalog). Below are services and solutions that our clients have deployed to include:

- Infor
- Splunk Enterprise

- Attunity CloudBeam for Amazon S3
- Attunity CloudBeam for Amazon Redshift (Premium) - BYOL
- Cloudberry Backup Server Edition
- Cloudberry Drive
- CloudCheckr
- Skeddly
- ESRI ArcGIS Online
- Cloud Protection Manager Enterprise Edition
- LAMP Stack powered by Bitnami
- F5 BIG-IP Virtual Edition for AWS (BYOL)
- CentOS 6 (x86\_64)
- Couchbase Server - Community Edition
- Ubuntu Server 12.04 LTS
- Apache Tomcat/CentOS
- Apache Tomcat/Hibernate (R)/CentOS

For the current solicitation it is our vision that all of the above services (IaaS, SaaS, PaaS) will work in concert together. Attachment H – Identification of service Models, outline our risk and deployment models for our proposed services and solutions. Day1's expertise as an Advanced Consulting partner with AWS cloud technology products and services provide NASPO and Participating Entities a platform for change.

As SaaS and PaaS based solutions become more of the norm in the enterprise, our team will offer discrete solutions for Public Safety, Human Resources, Transportation, Health Care and Administrative IT.

Day1's vision will infuse governance, security, and compliant cloud solutions that will meet government requirements (e.g. FISMA, HIPPA, PCI, FERPA, CJIS). Our team will offer State specific marketplace concepts (portals) that will allow the enterprise to build, manage and deploy repeatable configurable architecture frameworks that will reduce the time for design and architecting, increase innovation, mitigate risk, reduce cost; while building approved applications that can meet the most stringent security posture.

Infor's cloud products deliver an integrated application suite hosted mainly on multi-tenant AWS servers. Infor's industry leading model offers a flexible hybrid model, where some functionality is served on-premise and some functionality is served from the cloud, providing customers with the flexibility and adaptability that they need. Infor's cloud products are served from state-of-the-art industrial data centers and deliver enterprise-level functionality for Enterprise Resource Planning, Customer Relationship Management, Enterprise Asset Management, Property Management, Expense Management, Hospitality Management, and Workforce Management.

Infor offers two different cloud-based payment options, as well as standard on-premise deployment and dedicated hosting options. These choices include a software-as-a-service (SaaS) subscription option, where Infor can host customers' applications on Infor servers, and customers can receive pay-as-you go term licenses that enable

flexibility for on-demand software, as well as a hosted license option, where the customer purchases a perpetual software license, and we host the applications on our platform.

## 1.7 (E) 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.*

Day1 believes that NASPO requires a cloud vendor to have fully developed AWS capabilities to ensure that NASPO purchasing entities have a clear understanding of their responsibilities in a cloud operating model. There are four important basics regarding data security in the shared responsibility model:

1. Customers continue to own their data.
2. Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
3. Customers can download or delete their data whenever they like.
4. 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.

As an AWS partner we offer our clients/customers access to a significant list of AWS best practices, security frameworks, certifications, and compliance standards. The list below provides customers with the security standards, which work with the AWS Shared Security model that outlines the responsibilities for security and compliance in a customer environment. The AWS cloud infrastructure has been designed and is managed in alignment with regulations, standards, and best practices. The following list includes security, and industry certifications attained by AWS:

Federal Risk and Authorization Management Program (FedRAMP)	ISO 27018	National Institute of Standards and Technology (NIST) 800-171
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)	ISO 9001	International Traffic in Arms Regulations (ITAR)
SOC 2	Department of Defense (DoD) Security Requirements Guide (SRG) security impact levels 2 and 4	Federal Information Processing Standard (FIPS) 140-2
SOC 3	Federal Information Security Management Act (FISMA)	Family Educational Rights and Privacy Act (FERPA)



Payment Card Industry Data Security Standard (PCI DSS)	US Health Insurance Portability and Accountability Act (HIPAA)	Information Security Registered Assessors Program (IRAP) (Australia)
International Organization for Standardization (ISO) 27001	FBI Criminal Justice Information Services (CJIS)	IT-Grundschutz (Germany)
ISO 27017		

Day1’s Managed Services Program (MSP) provides NASPO full systems support; we maintain cloud architecture leaving NASPO purchasing entities to focus on using it. In addition to all security and management features included in Advanced Support, we manage critical tasks including configuration, patches, updates, and troubleshooting. We continually and proactively monitor your system to track key metrics, maintain maximum uptime, and provide notification should issues arise. Managed Services is ideal for clients wishing to take advantage of the cost savings and flexibility of a cloud environment without taking on security, system, and applications management. Pricing for Managed Services may vary and is based on the complexity of the cloud environment including architecture, number of servers, operating system, software, and usage.

The workflow process shown below is a high-level overview of our Managed Services workflow and shows how security is integrated into our daily operations. This also provides insight into how our team provides clearly defined in managing the security and maintenance of systems and applications in the cloud.

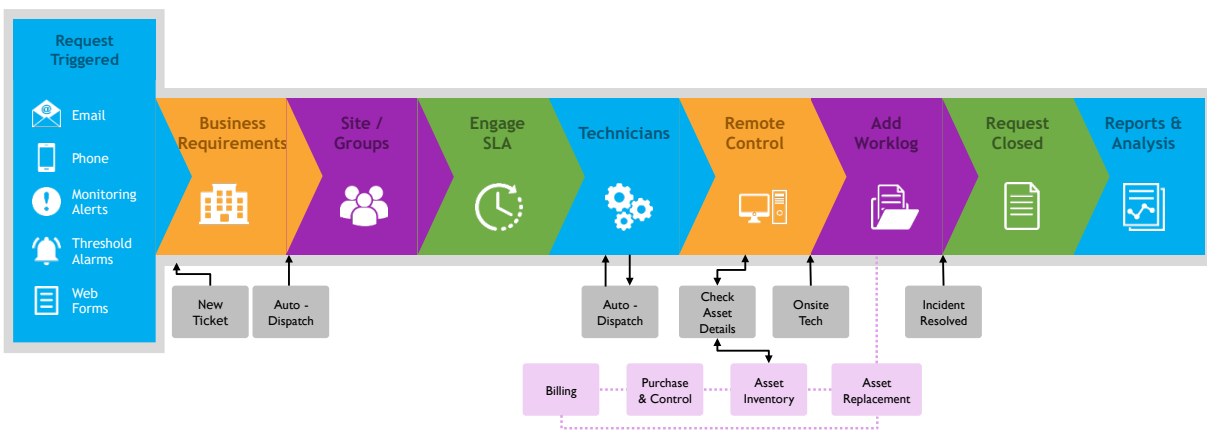


Figure 11: Processes for MSP

As identified above Day1 will leverage AWS Shared Responsibility model. This model provides important delineations that ensure that certain security measures, such as basic distributed denial of service (DDoS) protection and password brute-force detection are the defined. For instance, AWS provides protection on infrastructure components and ensures that they continuously scanned and tested. While some organizations perform vulnerability scanning on their resources once a quarter or once a month, Day1 provides customers with the ability to scan multiple times a day through AWS.

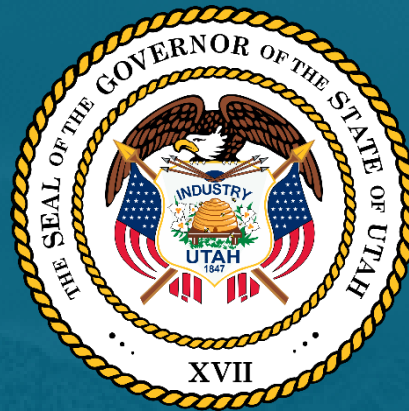
With automated tools, Day1 can enforce important security principles like least privilege and role segregation programmatically. Day1 can set custom metrics thresholds for unusual activity and automatically alert appropriate security experts or take the appropriate actions.

Day1 Solutions shall leverage best practices and procedures implemented by our partner AWS. AWS cloud infrastructure is housed in AWS's highly secure data centers, which utilize state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. All personnel must be screened when leaving areas that contain customer data. Data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. Independent auditors regularly evaluate the AWS Xen hypervisor security during assessments and audits.

The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, Payment Card Industry (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 Data Security Standard (DSS) version 2.0 published in October 2010. AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within an Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let customers take full advantage of the benefits of Amazon VPC and the AWS cloud while isolating Amazon EC2 compute instances at the hardware level.

AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems. Day1 Solutions can provide the support, patching above the hypervisor under our managed service program.



State of Utah Division of Purchasing

## NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTION

CH16012

# MANDATORY MINIMUMS



# Contents

1.0	Mandatory Minimums [RFP Section 5].....	2
-----	---	---

## 1.0 Mandatory Minimums [RFP Section 5]

*This section should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.*

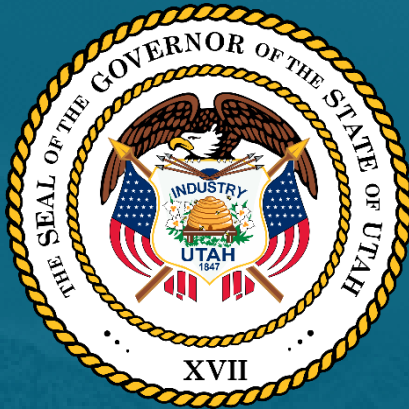
Minimum Requirement	Response Location	Yes Or No / Certifying Statement
<p><b>5.2 (M) Cover Letter</b> Proposals must include a cover letter on official letterhead of the Offeror; with the Offeror's name, mailing address, telephone number, facsimile number, e-mail address, and name of Offeror's authorized signer. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed.</p>	<p><b>Cover Letter</b></p>	<p><b>Yes.</b> Day1 Solutions has provided a cover letter including all company information and an authorized signature.</p>
<p><b>5.2.1 (M) Additional Terms and Conditions</b> 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.</p>	<p><b>Cover Letter</b></p>	<p><b>Yes.</b> Day1 Solutions understands that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.</p>
<p><b>5.2.2 (M) Proposal</b> A statement naming the firms and/or staff responsible for writing the proposal.</p>	<p><b>Cover Letter</b></p>	<p><b>Yes.</b> Day1 Solutions was solely responsible for writing the proposal. However, Amazon Web Services (AWS) provided marketing material in the form of a Partner Package.</p>
<p><b>5.2.3 (M) Federal or state procurement or non-procurement programs</b> A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.</p>	<p><b>Cover Letter</b></p>	<p><b>Yes.</b> Day1 Solutions is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.</p>

Minimum Requirement	Response Location	Yes Or No / Certifying Statement
<p><b>5.2.4 (M) NASPO ValuePoint Administrative Fee</b> 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.</p>	<p><b>Cover Letter</b></p>	<p><b>Yes.</b> Day1 Solutions acknowledges that a 0.25% NASPO ValuePoint Administrative Fee will apply to total sales for the Master Agreement(s) awarded from the RFP.</p>
<p><b>5.2.5 (M) Service model(s)</b> 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.</p>	<p><b>Cover Letter</b></p>	<p><b>Yes.</b> Day1 Solutions is capable of providing an expansive array of IaaS, PaaS and SaaS services through AWS with a unique ability to offer these in private, public or hybrid cloud environments. Today, under our existing contract we offer all service models in partnership with AWS core framework (compute, storage, and network). We then offer our clients the ability to layer in PaaS and SaaS based solutions from the AWS Lambda, code deploy, and Marketplace. Finally, we provide PaaS based offerings such as Lambda, code deploy, EC2 Containers to name a few.</p>
<p><b>5.2.6 (M) Data risk categories</b> A statement identifying the data risk categories that the Offeror is capable of storing and securing.</p>	<p><b>Cover Letter</b></p>	<p><b>Yes.</b> Day1 will leverage AWS US East and US West regions which hold a Provisional Authorization for level 2 which permits mission owners to deploy public, unclassified information in these regions with both the AWS Authorization and the mission application's ATO. The AWS GovCloud (US) region now holds a Provisional Authorization for levels 2 and 4 and permits mission owners to deploy the full range of controlled, unclassified information categories covered by these levels.</p>
<p><b>5.3 (M) Acknowledgement of Amendments</b> If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive.</p>	<p><b>Amendment Acknowledgement Form</b></p>	<p><b>Yes.</b> Day1 Solutions has acknowledged all amendments and provided a signed acknowledgment form for each amendment as required.</p>

Minimum Requirement	Response Location	Yes Or No / Certifying Statement
<p><b>5.5 (M) General Requirements for the Service Offerings</b></p>	<p><b>Organization Profile, Mandatory Minimums, and Technical Response</b></p>	<p><b>Yes.</b> Day1 Solutions complies with all General Requirements for the service offerings as outlined in the sections below and throughout our proposal as a whole.</p>
<p><b>5.5.1 (M) Usage Report Administrator</b> 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.</p>	<p><b>Organization Profile 1.0</b></p>	<p><b>Yes.</b> Day1 Solutions certifies that Bob Vuong, Vice President of Programs and Services will be the Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.</p> <p>His qualifications include:</p> <ul style="list-style-type: none"> <li>• Over 18+ years of experience in consulting and IT project management</li> <li>• 10+ years in building up systems integration capabilities at major consulting firms such as Booz Allen Hamilton and Northrop Grumman Corporation</li> <li>• Established Day1's organizational processes around program management services and delivery</li> <li>• Project Management Institute certified Project Management Professional (PMP)</li> </ul>
<p><b>5.5.2 (M) Ordering Instructions</b> 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.</p>	<p><b>Mandatory Minimums</b></p>	<p><b>Yes.</b> Day1 Solutions agrees to continue to cooperate with NASPO Value Point and SciQuest with uploading ordering instructions.</p>

Minimum Requirement	Response Location	Yes Or No / Certifying Statement
<p><b>5.5.3 (M) CSA STAR Registry Self-Assessment</b> Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment . Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.</p>	<p><b>Attachment B</b></p>	<p><b>Yes.</b> Day1 Solutions certifies that all control self-assessment data provided in Exhibit 1 and Exhibit 2 for our IaaS and SaaS offerings is current and up to date.</p>
<p><b>5.5.4 (M) Sample SLA</b> 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.</p>	<p><b>Technical Response</b> <b>1.4.1, 1.4.2, 1.10.2, 1.12.1, 1.12.2, Figure 44, Figure 45 and Figure 46</b></p>	<p><b>Yes.</b> Day1 Solutions can pass along AWS specific SLAs to NASPO purchasing entities, which AWS currently provides Service Level Agreements (SLAs) for several products. Section 1.12.2 of our Technical Response provides a sample list of these SLAs.</p>
<p><b>5.8 (M) Recertification of Mandatory Minimums and Technical Specifications</b> 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.</p>	<p><b>Mandatory Minimums</b></p>	<p><b>Yes.</b> Day1 Solutions acknowledges that if awarded a contract under this RFP that we will annually certify to the Lead State that it still meets or the technical capabilities discussed in its proposal.</p>





State of Utah Division of Purchasing

# NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTION

CH16012

## EXECUTIVE SUMMARY



# Contents

1.0	Executive Summary [RFP Section 5.4] (2 page max) .....	2
1.1	Day1 and WSCA's History .....	2
1.2	WSCA Transforms GIS to Cloud Strategy & Consultation.....	3
1.3	Evolving NASPO ValuePoint .....	3
1.4	Major Features of the Day1 Proposal .....	3

## 1.0 Executive Summary [RFP Section 5.4] (2 page max)

---

Day1 Solutions, Inc (Day1) has a unique history with NASPO Western States Contracting Alliance (WSCA) and in the cloud industry dating back several years. Day1 currently utilizes the WSCA Public Cloud Hosting contract to promote cloud adoption at the enterprise level in government agencies nationwide. With the largest number of Participating Addenda out of any prime vendor, Day1 is authorized to work with agencies in 14 states and is currently engaged with a number of others to help them realize the benefits of cooperative purchasing. It is our belief that streamlining the procurement process will enable agencies to quickly realize the speed, agility, and benefits of cloud computing, which will in turn provide a more agile development methodology to deploy innovative solutions and applications for constituents. We feel this provides us an unmatched perspective that is aligned with the goals of NASPO ValuePoint. We capture the essence of our cloud-centric solutions in this proposal in the three areas below that touch on the evolution of cloud through our extensive experience with the past, strong engagements in the present, and forward-leaning guidance towards the future of cloud for state, local, and education through NASPO ValuePoint Master Agreement for Cloud Solutions.

### 1.1 Day1 and WSCA's History

---

Day1 has a long history with NASPO WSCA, even dating back before Day1 was formed. Day1's Founder & CEO, **Mr. Luis Benavides**, was a member of Amazon Web Services (AWS) Worldwide Public Sector, which included a team working with State and Local Government (SLG) customers; Mark Fox, Eric Sheetz, Greg Duncan, and eventually Steven Halliwell. This AWS team was originally approached in May of 2011, for the "**Multi-State Cloud RFI Workshop**" held June 14<sup>th</sup> & 15<sup>th</sup> in Helena MT, invited by the Geographic Information Officer of Montana. This workshop, initially focused on GIS, included the original states behind the creation of WSCA Public Cloud Hosting Services: Montana (**Robin Trenbeath**), Utah (**Spencer Jenkins**), Colorado (**Jon Gottsegen**), Oregon (**Sean McSpaden**), and **Paul Stembler** the coordinator of NASPO WSCA. The goal of the WSCA states were to introduce the benefits of cloud computing in order to gain cost efficiencies, flexibility & scalability, and reduction in staff support time. It was Mr. Benavides' role at AWS to develop and build the AWS partner ecosystem. As it relates to WSCA, he worked directly with Dewberry Inc. who was teamed with Skygone Inc., Lockheed Martin Inc., as well as ESRI Inc. and Unisys Inc. The AWS team, including Mr. Benavides, wrote guidelines outlining the pricing models and AWS Security Best Practices to show how they could be adopted for the WSCA RFI. Mr. Benavides played a key role on the AWS team that assisted the partners in submitting their proposals for what was eventually the WSCA Public Cloud Hosting Services award in January 2013, almost two years after the initial workshop in Montana.

Day1 made a strategic decision to acquire the contract from Dewberry in November of 2014. Day1 was also a services partner to Dewberry for AWS during this time which helped develop an even closer relationship to both Dewberry and WSCA. Additional Day1 members also have history and continuity; **Ms. Sarah Sleyman**, who continues working with WSCA customers on a daily basis as one of Day1's top AWS and GIS Solution Architects, and **Mr. Jon Hepner** (Sales Manager), formerly of AWS, has worked with WA, OR, MT, CO, AZ, and HI. This deep history from our technical staff, sales team, and executive leadership resonates throughout our proposal and provides NASPO with a trusted partner who understands the intent of the vehicle and how to quickly and efficiently onboard new Purchasing Entities as they adopt new IaaS, PaaS and SaaS offerings. Day1 is viewed in high regard by the WSCA customers and AWS, our "Customer Obsession Award" is evidence of this high satisfaction awarded by AWS in October 2015.

## 1.2 Growing GIS to Cloud Strategy & Consultation

Since contract novation, Day1 has been directly engaged with NASPO WSCA customers, and our breadth of solutions has grown exponentially. In our proposal Day1 demonstrates how cloud is a great tool for transformation, but simply procuring cloud with little value-add services and solutions will not fulfill that vision. We show how our current engagements and efforts help strongly position us as a partner for NASPO to continue providing unprecedented services to Purchasing Entities. In our proposal we provide examples of how Day1 currently provides value-add services to help our current NASPO WSCA customers through their journey to private, hybrid, community, or public cloud. Throughout our proposal we provide examples of our active participation and relentless efforts on this vehicle as evident through our 14 Participating Addenda's. Comparatively, the other 3 remaining NASPO Public Cloud Hosting Services prime contract holders are massive organizations Unisys, Dell Marketing, and ESRI. During the time of proposal submission, they have 6, 5, and 5 Participating Addenda's respectively.

## 1.3 Evolving NASPO ValuePoint

As the cloud industry continues to mature, customers better understand what they want and can make better decisions on choosing their best path. If it's forging ahead and taking the initiative themselves or with the guidance of a firm like Day1, their goals are becoming more achievable with the successful adoption of cloud. Just as the consumer has evolved, so has NASPO in its service offerings as evident from the simple word change in the solicitation for "Cloud Services" to "Cloud Solutions". Day1 Solutions is a born in the cloud company focused on delivering best in breed cloud based solutions. We are more agile than the old guard of companies where cloud has become an ancillary offering. We are highly regarded because of our dedicated focus on cloud, it's not a business unit lost in a larger company, it's what we do day in and day out. Our own evolution can be found throughout our proposal as we describe new frameworks and methodologies for consulting, and new capabilities such as training. Additionally, these last few months we have closed more PA's than any other NASPO Public Cloud Hosting Services MA265 awardees; and as an evolved company, has been awarded more than 15x the value of contracts versus Dewberry at time of novation.

### NASPO AND PURCHASING ENTITIES EXPERIENCE

With the largest number of Participating Addenda (14) out of any prime vendor, Day1 is authorized to work with states and education entities such as Alaska, Arkansas, Colorado, Delaware, Hawaii, Maryland, University Maryland University College, Minnesota, South Dakota, Utah, and Florida.

## 1.4 Major Features of the Day1 Proposal

In this proposal you will read three main themes that resonate; we have strong past performance experience with WSCA Cloud, we have strong credentials in supporting customers journey to the cloud, and we continue to evolve our solutions with mature frameworks and methodologies. It will be clear that Day1 understands the needs and requirements of the evolving NASPO ValuePoint customer.

The customers have defined the requirements, NASPO is managing them, and Day1 stands ready to deliver. We look forward to continue helping our WSCA customers challenge the status quo and transform government.













































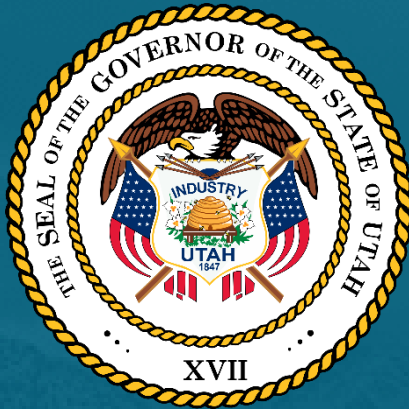












State of Utah Division of Purchasing

# NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTION

CH16012

## COVER LETTER



# Contents

1.0 Cover Letter [RFP Section 5.2] .....2

## 1.0 Cover Letter [RFP Section 5.2]

*Proposals must include a cover letter on official letterhead of the Offeror; with the Offeror's name, mailing address, telephone number, facsimile number, e-mail address, and name of Offeror's authorized signer. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed.*

Below provides the requested corporate information and our statements requested in section 5.2 of the RFP.

Day1 Solutions Information Sheet	
<b>DUNS:</b>	078470047
<b>Tax ID</b>	45-4982928
<b>CAGE:</b>	6R3U3
<b>Address Line 1:</b>	1751 Pinnacle Drive, Suite 425
<b>City:</b>	McLean
<b>State:</b>	Virginia
<b>ZIP/Postal Code:</b>	22102
<b>Corporate URL:</b>	www.day1solutions.com
<b>Fax #</b>	240-556-0200

Day1 Solutions certifies the following statements below:

- 5.2.1 Day1 Solutions understands that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.
- 5.2.2 Day1 Solutions was solely responsible for writing the proposal. However, Amazon Web Services (AWS) and Infor provided marketing material in the form of a Partner Package.
- 5.2.3 Day1 Solutions is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.
- 5.2.4 Day1 Solutions acknowledges that a 0.25% NASPO ValuePoint Administrative Fee will apply to total sales for the Master Agreement(s) awarded from the RFP.
- 5.2.5 Day1 Solutions is capable of providing an expansive array of IaaS, PaaS and SaaS services through AWS with a unique ability to offer these in private, public or hybrid cloud environments. Today, under our existing contract we offer all service models in partnership with AWS core framework (compute, storage, and network). We then offer our clients the ability to layer in PaaS and SaaS based solutions from the AWS Lambda, code deploy, and Marketplace. Finally, we provide PaaS based offerings such as Lambda, code deploy, EC2 Containers to name a few.
- 5.2.6 Day1 will leverage AWS US East and US West regions which hold a Provisional Authorization for level 2 which permits mission owners to deploy public, unclassified information in these regions with both the AWS Authorization and the mission application's ATO. The AWS GovCloud (US) region now holds a Provisional Authorization for levels 2 and 4 and permits mission owners to deploy the full range of

controlled, unclassified information categories covered by these levels.

As part of its commitment to transform enterprise and government through the use of innovative new technologies, The State of Utah, in conjunction with NASPO ValuePoint is looking to procure services for Infrastructure as a Service (IaaS), Software as a Service (SaaS) and Platform as a Service (PaaS) solutions. These cloud-based solutions will help state and local government revamp legacy business systems, processes and solutions that have previously been cumbersome and time consuming to implement on-premise. Through the use of IaaS, SaaS and PaaS, NASPO affiliated agencies and municipalities will benefit from the elasticity and scalability of the cloud, freeing up technical resources to focus on mission-critical systems, servicing the needs of constituents and expediting time-to-market for new applications. This transformation of government to a digital business will not be without its roadblocks. Utilizing a quick turnaround time for this solicitation, NASPO has put the ultimate test to vendors to see who can rise to the call and deliver comprehensive solutions, support and guidance while managing the needs of multiple state and local customers.

Day1 Solutions, Inc. (Day1) is pleased to submit our response to the State of Utah in conjunction with **NASPO ValuePoint Request for Proposal (RFP) solicitation #16012 - Cloud Solutions**. Day1 is an emerging industry leader representing a new breed in the Cloud Service Provider (CSP) model. As one of only four companies to currently hold and manage the current Western States Contracting Alliance (WSCA) Public Cloud Hosting Services contract from its inception, we have extensive experience guiding state, local and educational institutions on best-practices when adopting cloud solutions. This extensive experience allows for Day1 to appropriately translate all of our lessons learned from managing, operating, and delivering on the original WSCA contract vehicle to ensure success of NASPO ValuePoint Master Agreement for Cloud Solutions.

With the largest number of Participating Addenda out of any prime vendor, Day1 is authorized to work with agencies in 14 states and is currently engaged with a number of others to help them realize the benefits of cooperative purchasing. It is our belief that streamlining the procurement process will enable agencies to quickly realize the speed, agility and benefits of cloud computing, which will in turn provide a more agile development methodology to deploy more innovative solutions and applications for constituents. We feel this provides us an unmatched perspective that is aligned with the goals of NASPO ValuePoint. NASPO requires a business partner with strong cloud services capabilities to guide, oversee, promote, expand and verify the activities associated with this contract vehicle over an extensive period of time. Day1 is purpose built to serve the needs of state, local, and university IT systems and business requirements and will stay agile, focused and committed, to delivering quick measurable results. Our elite organizational AWS certifications, business qualifications, and past performances provides NASPO with the necessary assurance that Day1 has the appropriate certifications, experience, and knowledge required to deliver the highest quality technical and professional cloud based services. Day1 will continue to leverage a combination of Amazon Web Services (AWS) and our organizationally approved cloud solutions from teaming partners to further NASPO ValuePoint's mission to bring best value, innovation and competition in the marketplace for all 50 states, the district of Columbia and the organized US territories, their political subdivisions and other eligible entities.



Thank you for the opportunity to respond to the above mentioned Request for Proposal. Should you have any questions relating to the technical, cost, or contractual matters regarding our response, please do not hesitate to contact, Luis, Day1's authorized signer, at [luis@daysolutions.com](mailto:luis@daysolutions.com) or 703-646-3291.

Sincerely,



Luis Benavides, CEO and Founder  
Day1 Solutions, Inc.  
[luis@day1solutions.com](mailto:luis@day1solutions.com) | 703-646-3291

ATTACHMENT E

## 1.0 Day1 MSP SLA Structure

Issue / Request	Bronze		Silver		Gold	
	Response	Avg. Resolution	Response	Avg. Resolution	Response	Avg. Resolution
<b>SL1</b>	2 Business Hours	30 minutes - 4 hours	1 hour	30 minutes - 4 hours	30 min	30 minutes - 4 hours
<b>SL2</b>	4 Business Hours	-	2 hours	4 - 8 hours	1 hour	4 - 8 hours
<b>SL3</b>	Next Business Day	-	Next Business Day	1 - 3 Business Days	4 hours	1 - 2 Business Days
<b>SL4</b>	Next Business Day	-	Next Business Day	1 - 5 Business Days	Next Business Day	1 - 3 Business Days
<b>New Implementation</b>	1 - 5 Business Days	Project Dependent	1 - 3 Business Days	Project Dependent	Next Business Day	Project Dependent

ATTACHMENT E

## 2.0 Day1 MSP Severity Level Descriptions

Severity Level	Symptoms	Business Impact
<b>SL1</b>	Production server or other mission critical system(s) are down and no workaround is immediately available.	All or a substantial portion of your mission critical data is at a significant risk of loss or corruption. You have had a substantial loss of service. Your business operations have been severely disrupted.
<b>SL2</b>	Major functionality is severely impaired.	Operations can continue in a restricted fashion, although long-term productivity might be adversely affected. A major milestone is at risk. Ongoing and incremental installations are affected. A temporary workaround is available.
<b>SL3</b>	Partial, non-critical loss of functionality of the software.	Impaired operations of some components, but allows the user to continue using the software. Initial installation milestones are at minimal risk.
<b>SL4</b>	General usage questions.	No significant business impact.

**AWS PUBLIC SECTOR ACCESS POLICY**  
(Last Updated July 21, 2015)

This AWS Public Sector Access Policy (“**Access Policy**”) governs your access to and use of the Services (as defined below) of Amazon Web Services, Inc. (“**AWS**”) provided to you by your systems integrator, reseller, or services provider (“**Provider**”). It sets out the additional rules, conditions and restrictions that apply to you or the entity you represent (“**you**”) for use of the Services. In this Access Policy, “**we**”, “**us**”, or “**our**” means AWS and any of its affiliates. Please see Section 8 for definitions of capitalized terms.

**1. Use of the Services.**

**1.1 Generally.** You are provided access to the Services by your Provider. Your use of and access to the Services are governed by the agreement between you and Provider. This Access Policy supplements the terms of such agreement and may be updated by us from time to time. AWS Service Level Agreements do not apply to your use of the Services. Your continued access to and use of the Services is conditioned on your compliance with all laws, rules, regulations, policies and instructions applicable to your use of the Services, including the Policies.

**1.2 Account Keys.** Provider may provide you with AWS account keys which will allow you to directly access the Services via Provider’s account(s). We are not responsible for any activities that occur under these account keys, regardless of whether the activities are undertaken by you, Provider or a third party (including your employees, contractors or agents) and we are also not responsible for unauthorized access to the account.

**1.3 Third Party Materials.** Through the use of Provider’s AWS account(s), you may have access to Third Party Materials, such as software applications provided by third parties, which are made available directly to you by other companies or individuals under separate terms and conditions, including separate fees and charges. Your use of any Third Party Materials is at your sole risk.

**2. Your Responsibilities**

**2.1 Your Materials.** You are solely responsible for the development, content, operation, maintenance, and use of Your Materials with the Services. For example, you are solely responsible for:

- (a) the technical operation of Your Materials, including ensuring that calls you make to any Service are compatible with then-current application program interfaces for that Service;
- (b) compliance of Your Materials with the Acceptable Use Policy, the other Policies, and the law;
- (c) any claims relating to Your Materials;
- (d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Materials violate such person’s rights, including notices pursuant to the Digital Millennium Copyright Act;
- (e) any action that you permit, assist or facilitate any person or entity to take related to this Access Policy, Your Materials or use of the Services; and
- (f) End Users’ use of Your Materials and the Services and ensuring that End Users comply with your obligations under this Access Policy and that the terms of your agreement with each End User are consistent with this Access Policy.

**2.2 Other Security and Backup.** You or Provider are solely responsible for properly configuring and using the Services and taking steps to maintain appropriate security, protection and backup of Your Materials, including using encryption technology to protect Your Materials from unauthorized access and routinely archiving Your Materials.

**2.3 End User Violations.** If you become aware of any violation of your obligations under this Access Policy by an End User, you will immediately terminate such End User’s access to Your Materials and the Services.

### 3. Service Interruption.

**3.1 General.** We may suspend the AWS account(s) through which you access the Services immediately if we determine your or an End User's use of the Services (i) violates the terms of this Access Policy (including the Acceptable Use Policy or Service Terms); (ii) poses a security risk to the Services or any other AWS customer, (iii) may harm our systems or the systems or Materials of any other AWS customer; or (iv) may subject us to liability as a result of any of the foregoing. We will provide notice of any suspension as soon as practicable to Provider, who is solely responsible for providing any notices to you under your agreement with them.

**3.2 Scope of Interruption.** To the extent practicable, we will (i) suspend your right to access or use only those instances, data, or portions of the Services that caused the suspension, and (ii) limit the suspension to those accounts that caused the suspension. If commercially feasible, access to the Services will be restored once the conditions or circumstances giving rise to the suspension have been removed or corrected. Nothing in this Section 3 will operate to limit your rights or remedies otherwise available to you against Provider under your agreement with them or applicable law.

### 4. Proprietary Rights

**4.1 Services.** As between you and us, we or our licensors own and reserve all right, title, and interest in and to the Services. You have the right to use the Services solely as a licensee of Provider in accordance with this Access Policy and the agreement between you and Provider. We have no obligation to provide the Service to you under this Access Policy, so you must look exclusively to Provider and your agreement with Provider regarding such obligation. Except as expressly provided in this Section 4, you obtain no rights to the Services, the AWS Materials or any Third Party Materials.

**4.2 Materials.** As a part of the Services, you may have access to AWS Materials and Third Party Materials, which may be subject to additional terms and conditions (including the Terms of Use and Apache Software License). By using those materials, you are subject to such additional terms. You are solely responsible for securing any necessary approvals for the download and use of such materials.

**4.3 Restrictions.** Neither you nor any End User may use the Services in any manner or for any purpose other than as expressly permitted by this Access Policy and the agreement between you and Provider. Neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the Services (except to the extent software included in the Services are provided to you under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the software included in the Services or apply any other process or procedure to derive the source code of any software included in the Services, or (c) access or use the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas. All rights and access granted to you with respect to the Services are conditioned on your continued compliance with this Access Policy, and you will immediately discontinue your use of the Services if you cannot comply with this Access Policy.

**4.4 Suggestions.** If you provide any Suggestions to us when using the Services, you hereby grant to AWS and its affiliates a perpetual, irrevocable, non-exclusive, worldwide, royalty-free right and license to reproduce, distribute, make derivative works based upon, publicly display, publicly perform, make, have made, use, sell, offer for sale, and import the Suggestions, including the right to sublicense such rights through multiple tiers, alone or in combination.

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

**5. Representations and Warranties.** You represent and warrant that (a) you and your End Users' use of the Services (including any use by your employees and personnel) will not violate this Access Policy; (b) you or your licensors own all right, title, and interest in and to Your Materials; (c) Your Materials (including the use, development, design, production, advertising, or marketing of your Materials) or the combination of your Materials with other applications, content or processes, do not and will not violate any applicable laws or infringe or misappropriate any third-party rights; and (d) your use of the Services will not cause harm to any End User.

**6. Disclaimers.** WE PROVIDE THE SERVICES ON AN "AS IS" BASIS TO PROVIDER. WE AND OUR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND TO YOU, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICES OR ANY THIRD PARTY MATERIALS, INCLUDING ANY WARRANTY THAT THE SERVICES OR THIRD PARTY MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY MATERIALS, INCLUDING YOUR MATERIALS OR THE THIRD PARTY MATERIALS, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

**7. Limitations of Liability.** YOU MUST LOOK SOLELY TO PROVIDER AND YOUR AGREEMENT WITH THEM REGARDING ANY CLAIMS OR DAMAGES RELATED TO THE SERVICES. WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) SUSPENSION OF YOUR USE OF OR ACCESS TO THE SERVICES, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICES, OR, (III) ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON; OR (B) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR MATERIALS OR OTHER DATA THAT YOU OR ANY END USER SUBMITS OR USES IN CONNECTION WITH THE SERVICES (INCLUDING AS A RESULT OF YOUR OR ANY END USERS' ERRORS, ACTS OR OMISSIONS).

## **8. Definitions.**

**"Acceptable Use Policy"** means the policy currently available at <http://aws.amazon.com/aup>, as it may be updated by us from time to time.

**"AWS Materials"** means Materials we make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Materials does not include the Services.

**"AWS Service Level Agreement"** means all service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time.

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

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

**"End User"** means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Materials; or (b) otherwise accesses or uses the Services through you.

**"Materials"** means software (including machine images), data, text, audio, video, images or other content.

**"Policies"** means the Acceptable Use Policy, the Terms of Use, the Service Terms, all restrictions described in the AWS Materials and on the AWS Site, and any other policy or terms referenced in or incorporated into this Access Policy.

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

**“Service Terms”** means the rights and restrictions for particular Services located at <http://aws.amazon.com/serviceterms>, as they may be updated by us from time to time.

**“Suggestions”** means all suggested improvements to the Services or AWS Materials that you provide to us.

**“Terms of Use”** means the terms of use located at <http://aws.amazon.com/terms/>, as they may be updated by us from time to time.

**“Third Party Materials”** means Materials made available to you by any third party on the AWS Site or in conjunction with the Services.

**“Your Materials”** means Materials you or any End User (a) run on the Services, (b) cause to interface with the Services, or (c) upload to the Services or otherwise transfer, process, use or store in connection with the Services.