Contract # AR2505

STATE OF UTAH COOPERATIVE CONTRACT

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

Quest Media & Supplies, Inc.		
Name		
5822 Roseville Rd.		
Address		
Sacramento	CA	95842
City	State	Zip

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

Contact Person Ryan O'Keeffe Phone #916-338-7070 Email Ryan_Okeeffe@questsys.com
Vendor #VC205828 Commodity Code #920-05

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

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

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

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

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

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

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

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

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

CONTRACTOR

Contractor's signature — October 4, 2016 Date

Tim Burke, President and CEO
Type or Print Name and Title

STATE

Director, Division of Purchasing — 10.5.16 Date

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

(Revision 16 June 2016)

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

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

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

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

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

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

---

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

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

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

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

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

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

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

10. Defaults and Remedies

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

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

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

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

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

13. Indemnification

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

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

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

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

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

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

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

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

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

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

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

16. Insurance

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

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

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

(2) CLOUD MINIMUM INSURANCE COVERAGE:

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

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

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

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

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

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment

of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

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

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

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

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

19. Ordering

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

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

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

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

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

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

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

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

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

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

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

20. Participants and Scope

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26. Records Administration and Audit.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32. Transition Assistance:

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

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

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

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

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

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

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

37. Governing Law and Venue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attachment B – Identification of Service Models

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

Service Model:	**Low Risk Data**	**Moderate Risk Data**	**High Risk Data**	**Deployment Models Offered:**
Saas	Yes	Yes	Yes	SaaS Data Analytics
IaaS				
PaaS				

Attachment C – 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.

Software as a Service **Discount % 50**

Infrastructure as a Service **Discount % ____**

Platform as a Services **Discount % ____**

Value Added Services **Discount % 10**

Additional Value Added Services:

Maintenance Services

Onsite Hourly Rate $ 205.00
Remote Hourly Rate $ 185.00

Professional Services

- **Deployment Services** — **Onsite Hourly Rate $ 205.00**, **Remote Hourly Rate $ 185.00**
- **Consulting/Advisory Services** — **Onsite Hourly Rate $ 205.00**, **Remote Hourly Rate $ 185.00**
- **Architectural Design Services** — **Onsite Hourly Rate $ 205.00**, **Remote Hourly Rate $ 185.00**
- **Statement of Work Services** — **Onsite Hourly Rate $ 205.00**, **Remote Hourly Rate $ 185.00**

Partner Services **Onsite Hourly Rate $ 205.00**, **Remote Hourly Rate $ 185.00**

Training Deployment Services **Onsite Hourly Rate $ 205.00**, **Online Hourly Rate $ 185.00**

2016 NASPO/VALUEPOINT

COST PROPOSAL

Quest®
TECHNOLOGY MANAGEMENT

Pondera

FDaaS
Fraud Detection as a Service

NASPO CLOUD SOFTWARE AS A SERVICE PRODUCT CATALOG – effective March 10, 2016

List Price Pondera FDaaS

Product Number	Product	Price / Month
	Quest/Pondera Cloud FDaaS Fraud Detection Software	
PS-FDAAS-01	*Pondera Fraud Detection as a Service* *1-100,000 program participants. For every 100,000 participants, another module is added.* *I.e. 400,000 beneficiaries would cost $326,000/month.*	**$81,500**
PS-FDAAS-AS	***Pondera Application Specific Cloud based Software as a Service Modules including, but not limited to:***	
PS-FDAAS-CT	*Case Tracker* *Per 100,000 program participants*	**$61,000**
PS-FDAAS-SS	*Super Search* *Per 100,000 program participants*	**$21,500**
PS-FDAAS-SM	*Social Media Analyzer* *Per 100,000 program participants*	**$10,500**
PS-FDAAS-NA	*Network Analyzer* *Per 100,000 program participants*	**$40,750**
PS-FDAAS-ED	*Executive Dashboard* *Per 100,000 program participants*	**$15,000**
	Quest/Pondera Premium Technical Support	
PS-PTS-OTSE	*Pondera Premium Support – Onsite Technical Support Engineer*	**$215/hr**
PS-PTS-STSE1	*Pondera Premium Support – Senior Technical Support Engineer*	**$180/hr**
PS-PTS-PTSE	*Pondera Premium Support – Product Technical Support Engineer*	**$160/hr**
PS-PTS-STSE2	*Pondera Premium Support – Staff Technical Support Engineer*	**$140/hr**
PS-PTS-ATSE	*Pondera Premium Support – Associate Technical Support Engineer*	**$105 /hr**
PS-QST-MTC	*Quest Remote Maintenance Services*	**$205/hr**
PS-QST-DEP	*Quest Remote Deployment Services*	**$185/hr**
PS-QST-ADV	*Quest Remote Advisory Services*	**$185/hr**
PS-QST-ARC	*Quest Remote Architectural Design Services*	**$185/hr**
PS-QST-SOW	*Quest Remote Statement of Work Services*	**$185/hr**
PS-QST-PRT	*Quest Remote Partner Services*	**$185/hr**
PS-QST-TDS	*Quest Online Training Deployment Services*	**$185/hr**

Maintenance renewals for software product purchases shall be fixed at the agencies prior applicable rates, with a 0% uplift (no up-lift) and no additional increases, fees or charges added, for the duration of our NASPO contract.

Quest/Pondera FDaaS	Discount % Government Naspo ValuePoint
1 Year Contract	**50%**
3 Year Prepaid Contract	**53%**
5 year Prepaid Contract	**55%**
Quest/Pondera FDaaS Support and Services	**Discount % Government Naspo ValuePoint**
All Support and Services hours	**10%**

Fraud Detection as a Service (FDaaS)
PS-FDAAS-01

Pondera's Detection Solutions are award-winning, modern analytics solutions designed to help you detect potential fraud, waste, and abuse. They detect both individual transaction anomalies, as well as trends, patterns, and clusters that may indicate suspicious or fraudulent activities.

Our Detection Solutions are:

- Comprehensive - Analyze every program participant, beneficiary, claimant and transaction
- Scalable - Proven performance on some of the country's largest programs
- Intuitive - Designed "by our investigators for your investigators"
- Proactive - Innovative "push analytics" sends Alerts to your staff

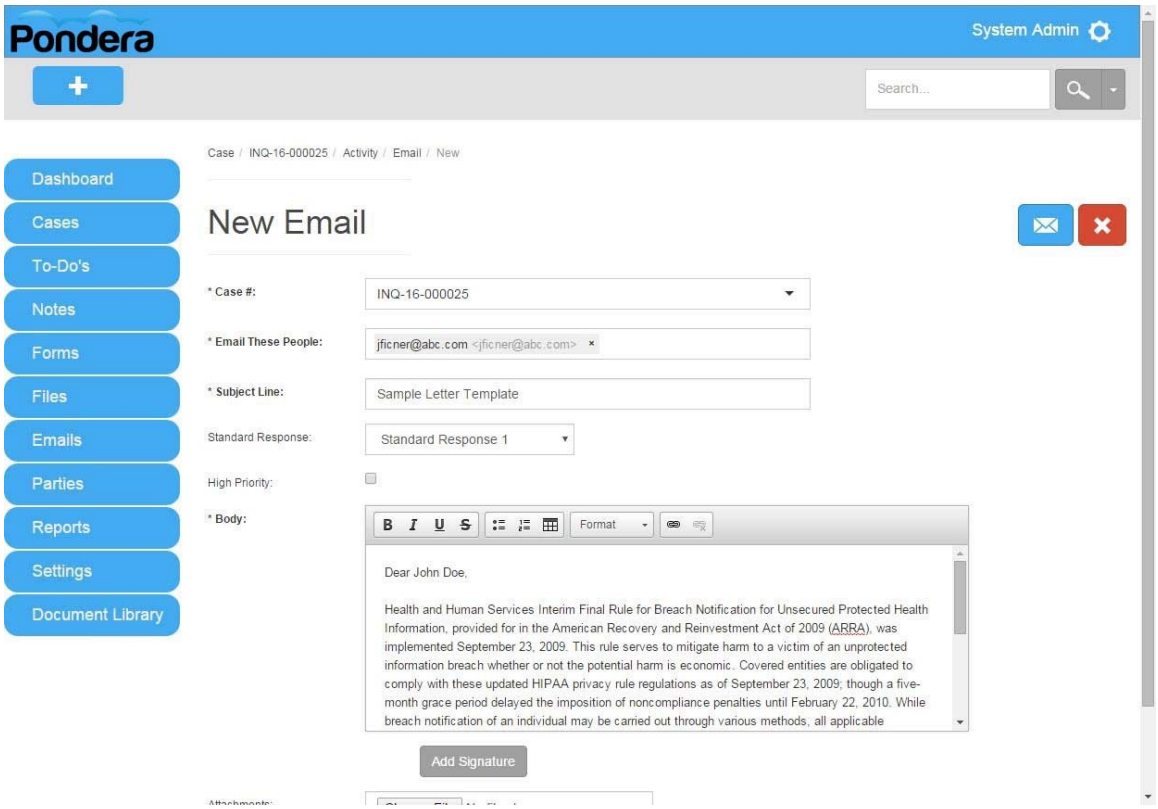
FDaaS is our core detection solution. FDaaS ingests your program data, matches it against third party data sources, and then runs it through a series of procedural and prediction models to detect previously known and unknown anomalies and patterns.

When a transaction violates a predetermined threshold, FDaaS sends an Alert to the integrated FDaaS Dashboard, Provider or Participant Profile, and Geospatial Analysis Maps. Your staff can view the Alerts, interact with the Maps, and create cases directly from the FDaaS system.

Cloud Solution Case Tracker
PS-FDAAS-CT

Pondera's Case Tracker is a fully-integrated investigative case tracking and management system. Case Tracker imports cases from FDaaS, or other sources, and uses workflow and rules engines to allow you to assign and route cases throughout their resolution process. The system also allows you to attached documents, images, and other files to your cases. Case Tracker can also automate activities such as sending an email to a program participant who is ineligible. It also includes a full reporting suite to track cases by investigator or division by month, quarter, or year.

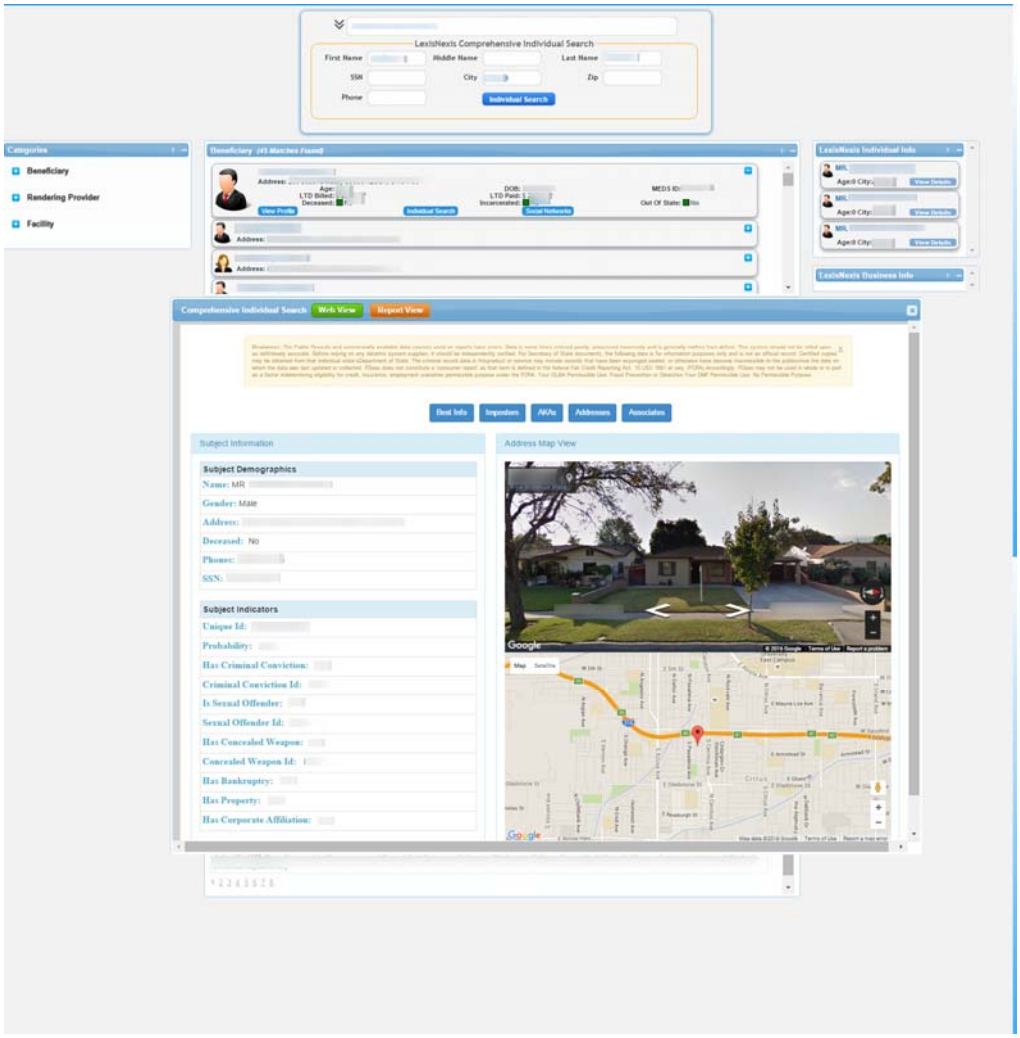
Case Tracker is bi-directionally integrated with FDaaS, receiving cases from FDaaS and returning results of investigations back to FDaaS to tune models and violation thresholds.



Cloud Solution Super Search *Premium*
PS-FDAAS-SS

SuperSearch *Premium* is a powerful, but easy-to-use, search tool that allows your investigators to type in a name or other word and search for matches in the FDaaS database and integrated third-party public records databases. Users can select categories (such as business, beneficiary, doctors, etc.) to narrow searches, and the search results link directly to the FDaaS profiles for more information.

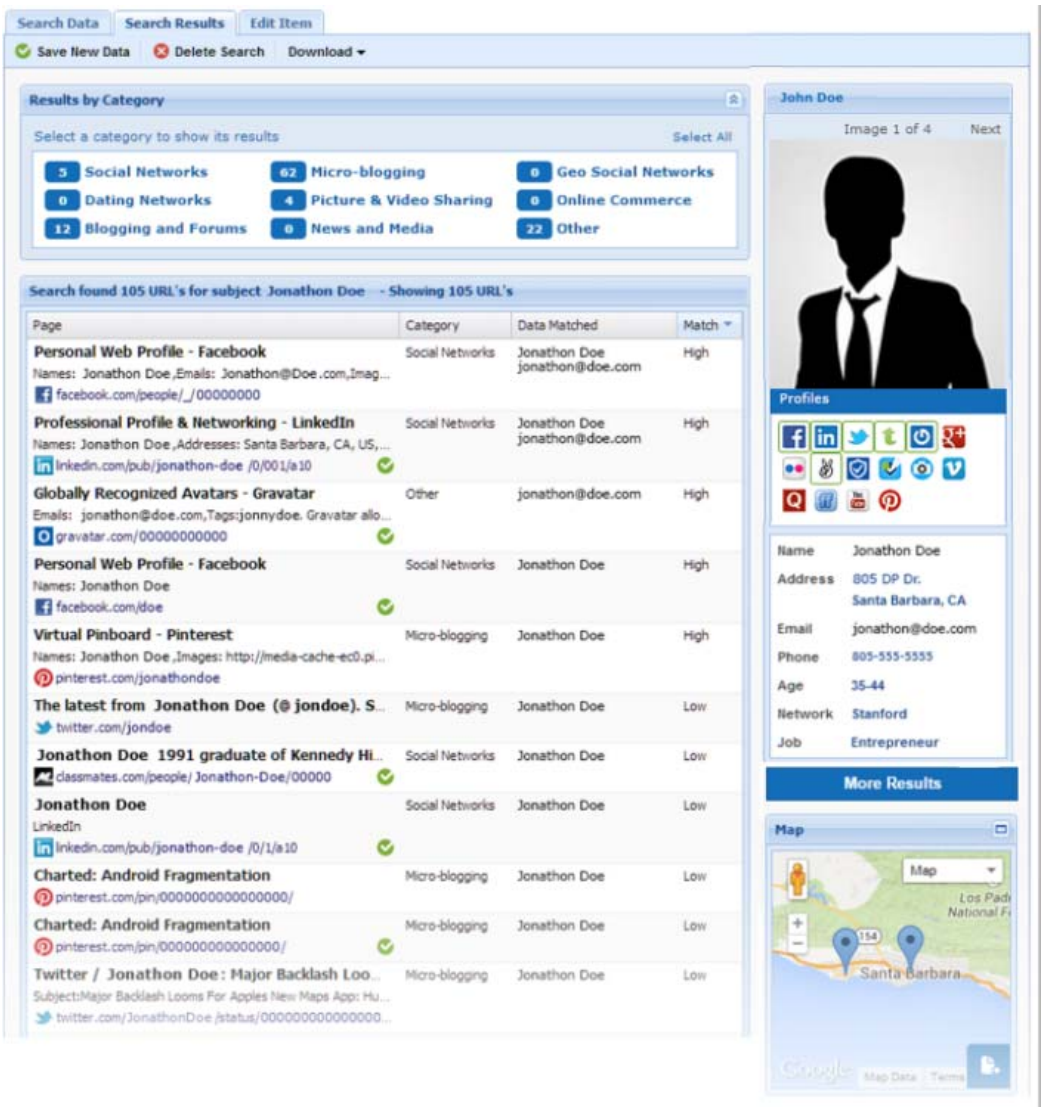
SuperSearch is an important investigative tool to quickly gather information on suspects. It is also fully integrated with third party public records and location information on individuals and businesses.



Cloud Solution Social Media Analyzer
PS-FDAAS-SM

Pondera's Social Media Analyzer, which can be accessed directly or through SuperSearch, is a powerful analysis tool that combs through social media sites such as blog posts, social networking sites, and other Internet sources where suspects may have left a digital footprint.

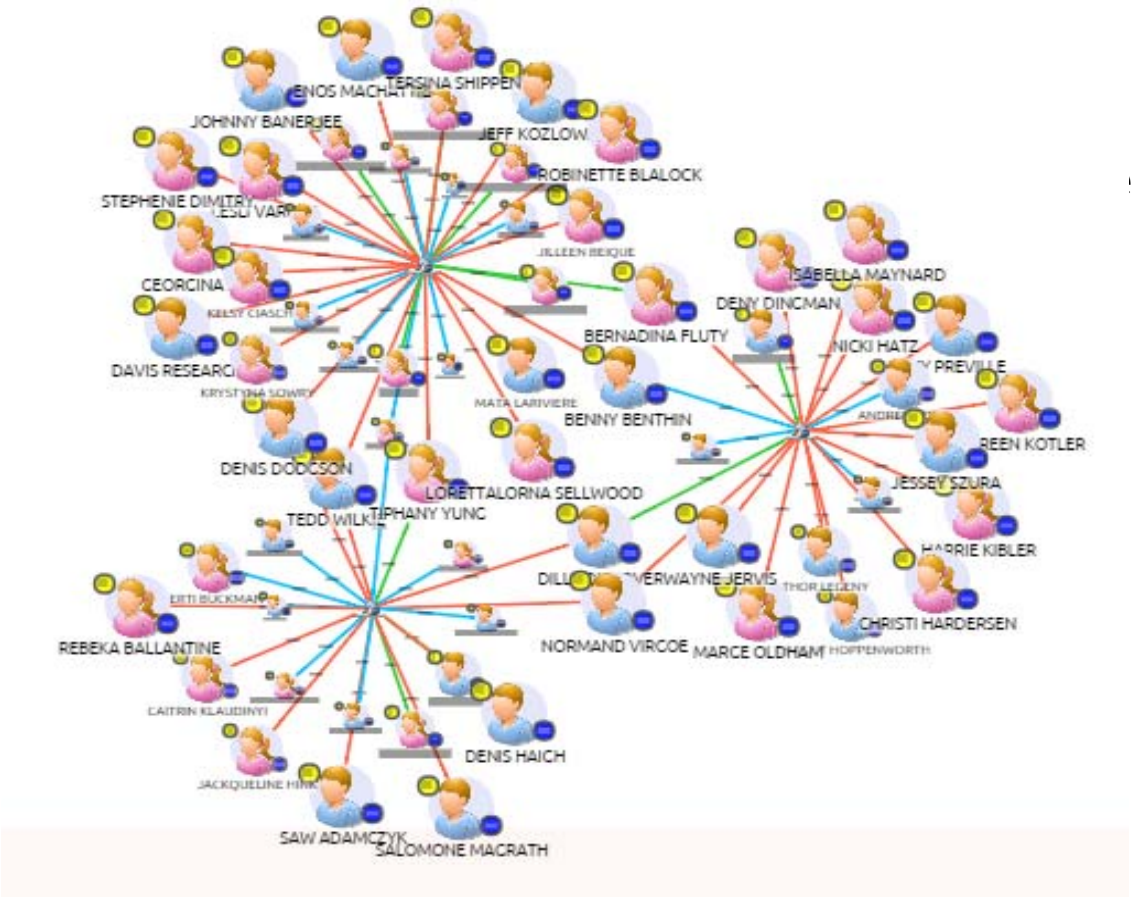
Using Social Analyzer, your analysts and investigators can uncover previously unknown connections and activities, such as illicit sales of government benefits. Analysts also use Social Media Analyzer to form a more complete picture of a suspect's relationships, behaviors, and activities.



Cloud Solution Network Analyzer
PS-FDAAS-NA

Network Analyzer is a powerful visualization tool that allows your investigators to explore and visualize relationships between and among program providers and beneficiaries. Network Analyzer is fully integrated with FDaaS allowing you to examine relationships such as shared program participants and unusual travel patterns.

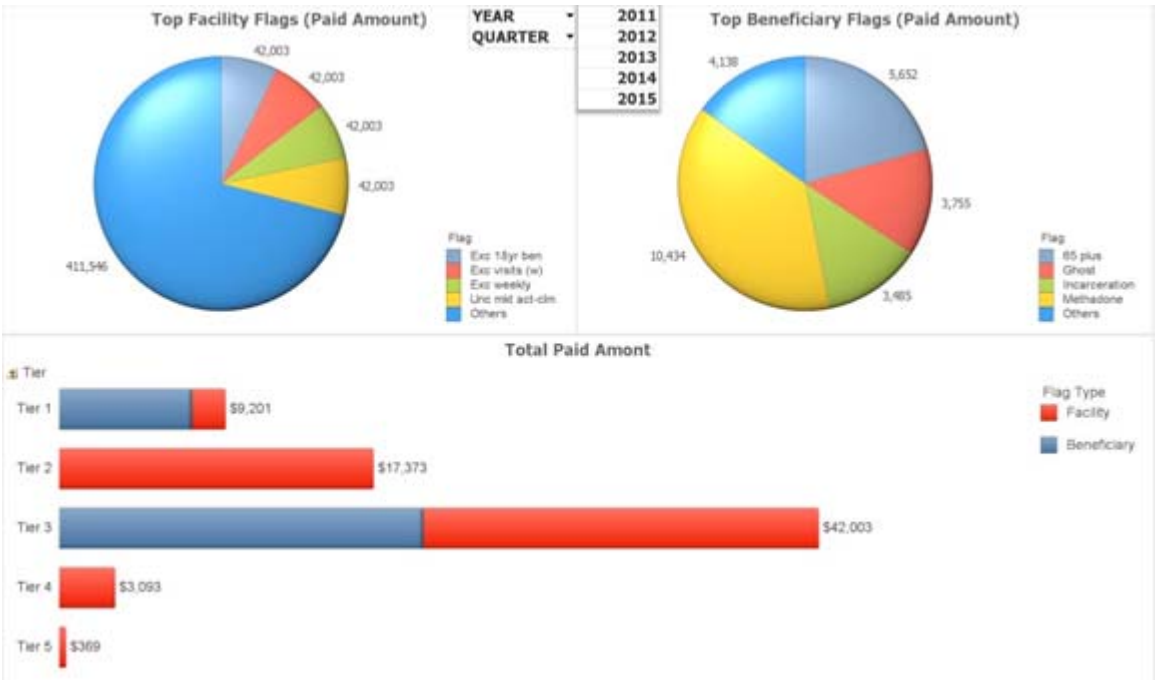
Network Analyzer comes pre-packaged with Network Templates that help you detect commonly used fraud schemes by simply running the out-of-the-box queries. It also allows more sophisticated users to create their own Network diagrams, add custom nodes and notes, and save or print the diagrams.



Executive Dashboard
PS-FDAAS-ED

Pondera's Executive Dashboard is an intuitive executive reporting system that displays results of the Pondera analytics to program and agency managers. The Dashboard displays results in pie charts, bar charts, and tables which pull data directly from the FDaaS database.

Dashboard users can drill through the charts to view changes over time, top flag violations, percentage increases, and other important program information. This helps management allocate program integrity resources and view the results of their enforcement actions.



Response to:
The State of Utah
Division of Purchasing
In conjunction with
NASPO/ValuePoint
Request for Proposal

Utah Solicitation Number CH16012

SaaS Data Analytics Solution

Prepared and Submitted by:

Quest®
TECHNOLOGY MANAGEMENT

March 8, 2016

Table of Contents

RFP Signature Page

5.1 Signature Page

Original signed copy submitted as part of this response.

State of Utah Vendor Information Form

Legal Company Name (include d/b/a if applicable)	Federal Tax Identification Number	State of Utah Sales Tax ID Number	
Quest Media & Supplies, Inc.	94-2838096	n/a	
Ordering Address	**City**	**State**	**Zip Code**
5822 Roseville Rd.	Sacramento	CA	95842
Remittance Address (if different from ordering address)	**City**	**State**	**Zip Code**
same as above	same as above	CA	same as above
Type ☐ Proprietorship ☐ Partnership ☐ Government ☒ For-Profit Corporation ☐ Non-Profit Corporation	Company Contact Person: Tim Burke		
Telephone Number (include area code): (916) 338-7070	Fax Number (include area code): (916) 338-3289		
Company's Internet Web Address: Questsys.com	Email Address: Tim_Burke@questsys.com		
Offeror's Authorized Representative's Signature: Tim Burke			
Type or Print Name: Tim Burke			
Position or Title of Authorized Representative: President and CEO			
Date: 3/4/2016			

Executive Summary

Quest Media and Supplies, Inc., hereafter referred to as Quest Technology Management, with our strategic partner Pondera Solutions (Quest/Pondera) is proposing our Fraud Detection as a Service (FDaaS) solution to meet the requirements of the NASPO SaaS Cloud Solutions RFP. The solution is housed at Quest's high level security data centers. Quest's nationwide Service Delivery Centers provide safe and secure cloud computing environments for any industry while meeting or exceeding regulatory requirements. Our goal is to offer purchasing entities the best possible cloud computing consulting and solution to fit each entities' needs and budget.

We have chosen to partner with Pondera Solutions to offer the premier Software as a Service – Data Analytics solution, "Fraud Detection as a Service, or FDaaS" to Participating Entities. The Quest/Pondera team combines premier data center solutions with best in class fraud detection software for government entities. Pondera's FDaaS is a modern, comprehensive Software as a Service (SaaS) application that is being used to **detect and prevent fraud by using advanced data analytics** in some of the largest state programs in the country.

FDaaS meets all of the requirements of this Cloud Solutions SaaS RFP and offers additional functionality such as Social Network Analysis and SuperSearch that exceed the requirements. While FDaaS is an existing product, it is also highly configurable to meet each State's unique requirements.

FDaaS offers the following advantages to the Participating Entities:

1. **Comprehensive, Integrated Functionality**: Including automated Alerting, Geospatial Maps, Link Analysis, Social Network Analysis, Fraud Indicators, Supervised and Unsupervised Prediction Algorithms, and more.

2. **Machine Learning**: Constant improvement through machine learning and human feedback mechanisms.

3. **Ease of Use**: A fully integrated Investigative Dashboard "designed by investigators for investigators".

4. **Secure Hosting**: A proven hosting process and facility with Quest that meets and exceeds required security standards including HIPAA.

5. **Integrated Implementation Methodology**: The Pondera Requirements and Onboarding Process (PROP), designed specifically for FDaaS implementations, leads to implementations in as few as 120 days.

6. **Virtual Special Investigations Unit (SIU):** Pondera's virtual SIU, consisting of certified fraud examiners, program experts, program integrity managers, and former federal and state law enforcement staff who remotely design the system, train your users, support the implementation, participate in your enforcement planning and review sessions, and deliver investigative reports.

FDaaS, as an existing cloud-based software as a service data analytics solution, drastically reduces implementation timelines and risk. Its configurability ensures that you receive a system customized to your specific requirements. Its ease-of-use makes a system that your users will quickly learn and use. And its self-learning capabilities will continue to improve over time to identify new and emerging fraud trends.

FDaaS is an existing solution that we will configure to meet each State and program's unique requirements. In the response to this RFP, we include a number of screenshots from the existing solution to illustrate existing functionality. Please note that we have scrambled or blocked any PII data in the screenshots.

FDaaS provides an intuitive dashboard with participant profiles, alerts, grids, and ScoreCards.

FDaaS is a true automated detection and alerting system, versus traditional Information Technology tools that require you to search for data anomalies. The system ingests your data, combines it with third party consumer and business data, and then runs every transaction through a set of procedural and prediction models and data analytics.

Pondera's FDaaS is being used in 5 states: California, Iowa, Georgia, Nevada and Pennsylvania and multiple programs that include Medicaid, Unemployment Insurance, SNAP, Tax and Revenue, and Integrated Eligibility.

Mandatory Minimums

5.2 Cover Letter

5.3 Acknowledgement of Amendments

Original signed document submitted with this response.

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

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

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

Quest Media & Supplies, Inc.

Offeror

Representative Signature

Tim Burke, President and CEO

5.5 General Requirements

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

Quest Technology Management certifies that we will provide a Usage Report Administrator responsible for the quarterly sales reporting described in the Master Agreement Terms and Conditions, and if applicable, Participating Addendums.

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

Quest Technology Management certifies that if awarded a contract, we agree to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions.

5.5.3 ***Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matric (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.***

Quest Technology Management agrees to complete, provide, and maintain a completed CSA STAR Registry Self-Assessment. We represent and warrant the accuracy and currency of the information on the completed forms. The completed CSA STAR Registry Self-Assessment is attached to the end of this response.

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

Quest Technology Management has provided a sample of our Service Level Agreement which defines the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

5.7 Recertification of Mandatory Minimums and Technical Specifications

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

Quest Technology Management acknowledges that if we are awarded a contract under the RFP, we will annually certify to the Lead State that we still meet or exceed the mandatory minimum requirements and technical specifications of the RFP.

Business Profile

6.1 Business Profile

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

Quest Technology Management is headquartered in Sacramento, California. Quest was founded in 1982 during the early days of the PC revolution. Large mainframe data centers formed the initial client base, buying mainly mainframe media, peripherals, PC products and supplies. Yet early on and based on demand, Quest founders Cindy and Tim Burke, envisioned a broader company – one that would help clients achieve their competitive business goals by serving all their technology needs.

Today, Quest is a privately-owned technology management firm that serves a diverse client base of Fortune 50-5000 corporations, state and local governments and educational institutions. The company offers clients a portfolio of computer hardware and networking equipment, professional services, cloud and managed services, telecommunications & transport, support & maintenance management, fiber-optics, wireless & structured cabling, and technical staffing, all backed by the most advanced technologies. Quest is a worldwide leader in technology management offering a portfolio of professional, Cloud, and Managed Services. Either on-site or from one of 25 secure global Service Delivery Centers, Quest offers Security, Disaster Recovery, Business Continuity, Data Backup and Replication, Desktops as a Service, and Infrastructure as a Service.

Quest has achieved significant growth over the past few years garnering awards to this effect most notably CRN Fast Growth 150 for the past two years, in addition to the MSP 500 and Tech Elite 250 resulting in Quest being awarded the CRN Triple Crown for two years running. Fewer than 60 North American solution providers had the necessary revenue, growth, and technical expertise to be recognized on three of CRN's preeminent solution provider lists, earning them the Triple Crown Award this year.

The company employs approximately 160 people, including teams of consultants, engineers, project managers, product specialists, customer service representatives, and administrative personnel focused on making Quest an industry leader by delivering the

latest in technology tools and services that best serves the business goals of the clients. Quest maintains a high employee retention rate – notably Quest's managers have at least 15 years with the company with more than a few service records include over 30 years. The listed contract manager for this engagement has more than 8 years of experience with Quest and each of the supporting team has 10 years or more.

Quest is an expert at private, public, and hybrid-cloud. We have been delivering private cloud computing solutions for over 10 years – leveraging the power of the internet to fulfill our clients' computing needs across their various locations. In fact, Quest delivered "Cloud Computing" before the term was coined. Quest offers cloud services for both the public and private sector in the form of Software as a Service (SaaS), Infrastructure as a Service (IaaS) and /or Platform as a Service (PaaS) to partners and customers.

Quest Technology Management's strategic partner, Pondera Solutions, is a Google Enterprise partner founded in 2011 and headquartered in Gold River, CA. Pondera is singularly focused on leveraging the power of cloud computing and advanced analytics to combat fraud, waste, and abuse in large government programs. Every Pondera employee is focused on this objective every day. This is all they do.

Pondera has three (3) divisions – Technology, Service Delivery, and Sales/Operations. Their current client base spans 5 states and 12 different government programs. Pondera has experienced 1500% revenue growth over the last three years and over 800% employee growth over the last three years. Pondera currently employs 45 people across two locations. The Pondera headquarters are located just east of Sacramento. Pondera's employee retention rate is 100%. Pondera has been providing cloud based data analytics for some of the largest programs in the country over the past 5 years. All of their implementations are for government agencies.

Pondera's flagship product, Fraud Detection as a Service (FDaaS) is a comprehensive solution designed to detect and alert you to potentially fraudulent Providers, Beneficiaries, and Claims. It also includes tools to help your analysts and investigators build a case for enforcement or prosecution.

Pondera's FDaaS is also "built by investigators, for investigators". They hire more than 50% of their employees directly from government. They leverage their knowledge and experience and encourage them to be creative and take risks in our research and

development functions. And they ask them to focus on delivering a solution that is powerful, yet easy to use, allowing you to focus on investigating and prosecuting cases versus learning how to use complex information technology tools.

At this time, Pondera works in 5 states that include California, Iowa, Nevada, Pennsylvania, and Georgia. Pondera works in many different programs, including, but not limited to: Medicaid, Unemployment Insurance, SNAP, Tax and Revenue, and Integrated Eligibility.

6.2 Scope of Experience

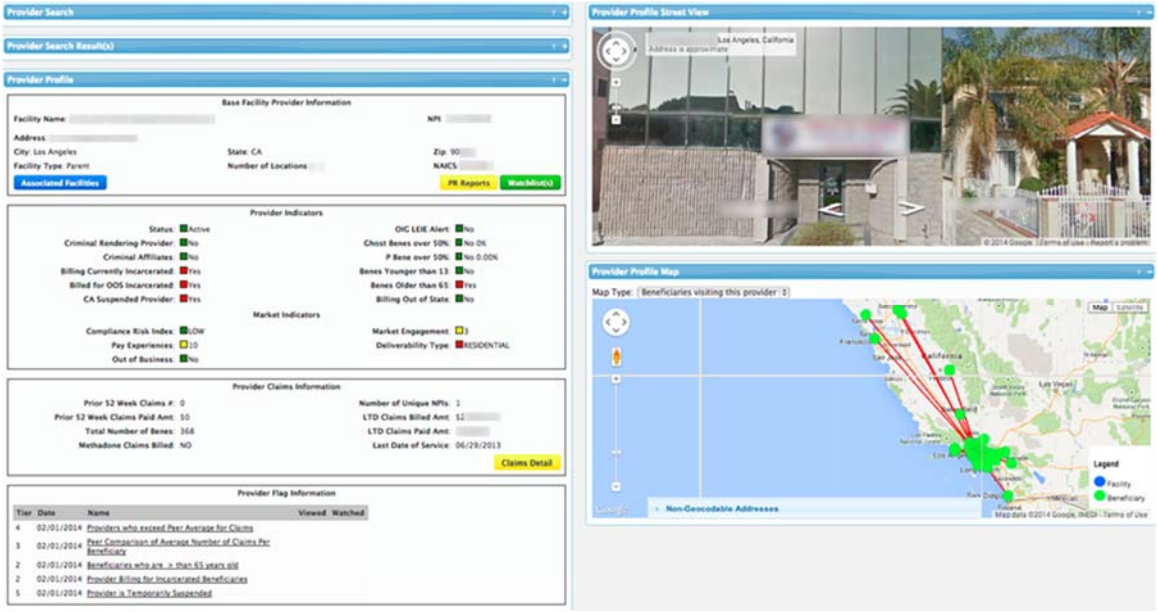
Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the Offeror provided solutions identical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

Quest Technology Management's strategic partner, Pondera Solutions, works exclusively in government programs. Quest Technology Management provides the hosting environment for all of Pondera's current implementations. Pondera's contracts are very similar to the Master Agreements that are sought through this RFP. In addition to the contracts listed below, Pondera participates on the California Software Licensing Program which is also a leveraged purchasing program. The SLP program is administered by the Department of General Services for the State of California. The total approximate dollar value of their 5 largest contracts in the last two years is $9,250,000. Under these contracts, Pondera provides their Fraud Detection as a Service (FDaaS) solution, the cloud based data analytics tool which we are offering through this RFP.

As an example of their deployments, we have included the details of 3 current implementations.

A. **California Department of Health Care Services**: **Substance Use Disorder Services – SaaS Cloud Data Analytics** (September 2013 – Present)

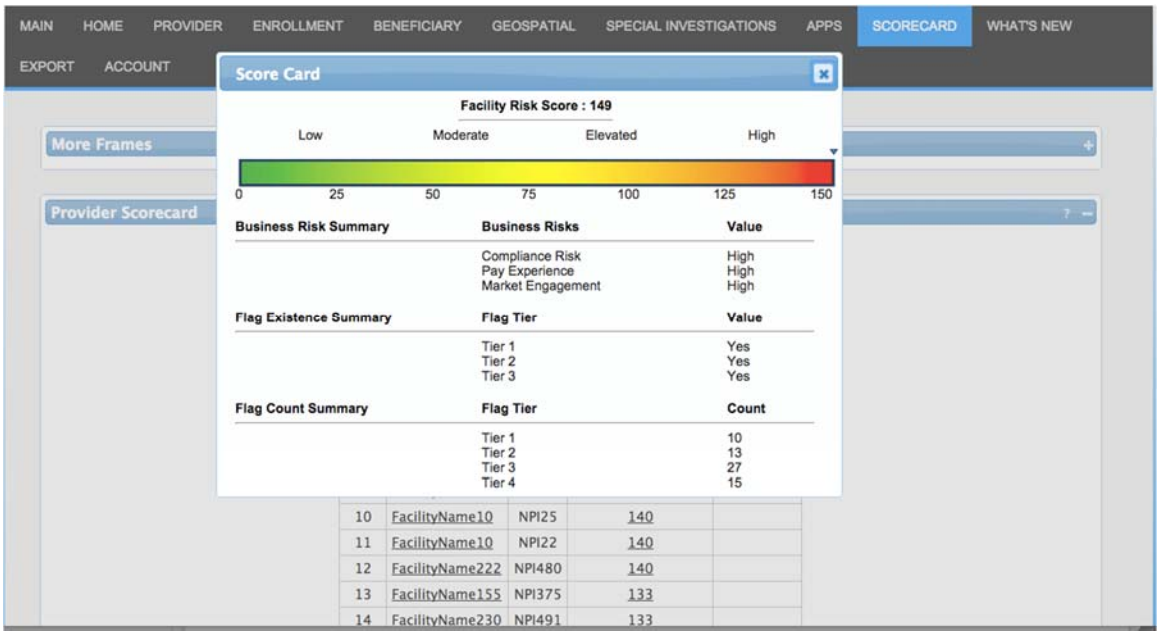
   Pondera was awarded the Short-Doyle Data Analytics project in 2013 to detect and help prevent fraud, waste, and abuse in the California Drug Medi-Cal program. The FDaaS system was implemented within three months of receipt of the client data, and is used to analyze Providers and Beneficiaries in the Medicaid drug and alcohol counseling programs. There are approximately 225,000 beneficiaries and 6,000 providers in the program.



A de-identified screenshot of a Provider Profile shows suspicious behaviors and critical business information.

The FDaaS Dashboard for this client displays Alerts, Geospatial Analysis, Link Analysis, Social Network Analysis, and Provider and Beneficiary Profiles. It integrates third party consumer and business data to detect issues with identity, eligibility status (such as age, out-of-state indicators, and incarceration status), and potential fictitious businesses (such as shell company activity, credit experience, and criminal histories). It also includes dozens of flags for program specific issues such as holiday billings, spike indicators, and other potential issues.

California DHCS also uses the integrated FDaaS Provider Scorecard which ranks and scores every Medi-Cal Drug Provider for the potential for fraud. The fraud scores are derived from the individual FDaaS flags and allow the DHCS Audits & Investigations (A&I) team to "stack rank" their providers to prioritize field audits. An actual screenshot of the California Scorecard (de-identified) is provided below.



CA DHCS uses the Scorecard to rank all facilities for fraud potential. This is a de-identified example of the detail behind one of the facilities' ranking.

DHCS also contracted with Pondera to analyze "cross-over" Beneficiaries who display suspicious activities across DHCS programs. For example, FDaaS is used to identify beneficiaries who are billed for a counseling session in one part of the state while also being billed for an in-hospital stay in another part of the state.

Pondera's Special Investigations Unit plays an active role on this project. They participate in weekly strike team meetings, analyze data sets and recommend new flags, train DHCS users, and deliver intelligence reports to support DHCS enforcement activities. They also assist DHCS in their meetings with law enforcement agencies.

B. **Iowa Workforce Development** (July 2013 – Present)

The Iowa Workforce Development (IWD) has used FDaaS since 2013 to identify potential fraud and abuse in the Iowa Unemployment Insurance (UI) program.

There are approximately 50,000 claimants and 100,000 employers. FDaaS generates fraud alerts and potential leads, instances of aberrant payments, filings, and other potential fraud indicators on UI claimants and employers. Pondera's Special Investigations Unit also provides enhanced investigative support for large, complex cases.

IWD has used FDaaS to enforce and prosecute various program violations including identity theft, incarcerated claimants, deceased applicants, and out-of-state fictitious businesses set up for the sole purpose of processing fraudulent claims. Iowa has renewed the service two separate times since the initial year of the contract.

C. **Nevada Department of Health and Human Services**

The Nevada Department of Health and Human Services – Division of Welfare and Support Services was awarded a $1.5M grant from the U.S. Department of Agriculture in October 2015. The grant will allow Nevada to deploy FDaaS to detect and manage cases of SNAP card trafficking. There are approximately 400,000 claimants and 2,000 retailers in the program.

The project is scheduled to go live in the first quarter of 2016.

6.3 Financials

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

The Quest audited financial statements are submitted with this response as 2013_YE.pdf and 2014_YE.pdf. Quest's Dun and Bradstreet number is 107550055 with credit rating 4A3.

6.4 General Information

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

Pondera's FDaaS solution is used in 5 states and across 16 different programs. All of their implementations are cloud Software as a Service implementations. Their

singular focus is Fraud, Waste, and Abuse in government programs. They have been recognized in numerous publications as a leader in data analytics and government technology. FDaaS is used to identify fraudulent behaviors in the program, and then prioritize these egregious violations for the investigators. FDaaS includes tools that assist investigators in their day to day work, managers in their oversight and support, and executives in their evaluation of resources and effectivity.

The FDaaS Dashboard is designed "by investigators, for investigators". Ease of use and a maximum of two clicks to data are the guiding principles of the design. The different FDaaS modules are integrated by hyperlinks allowing, for example, drill through from geospatial maps and Alerts to the Provider and Beneficiary Profiles. And we use plain English, written by our investigators, to describe Alerts and other system functionality.

FDaaS takes complex analysis and data and displays results in a number of user-friendly ways including:

1. SuperSearch returns "mini" profiles with aggregated program, 3rd party, social and financial data
2. Scorecards display risk scores and comparison reporting by category
3. Grids provide color-coded X,Y axis data grids
4. Geospatial Maps display participants with shared emails, phones, IP addresses, etc.
5. Profiles provide fraud indicators, flags, and billing and claims history for Providers, Facilities, and Beneficiaries
6. Network Analysis visually links entities

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

Quest prepares an SSAE 16 report annually which is audited by a third party. A copy is submitted as part of this response.

6.5 Billing and Pricing Practices

6.5.1 ***Billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entities.***

Our proposal includes a discount off of our list price. This price is very straightforward and applies to both our Software as a Service pricing for all modules as well as to the additional support hours that are available.

It is our preference to bill 20% of the annual cost at the time the contract is signed and then to collect the remaining 80% of the annual cost when the project goes live. We understand that every Participating Entity will have different needs apply to the billing practices and we have every intention of accommodating their requirements.

Billing will be done Net 30.

The pricing is built on the number of participants in the program. Because this is a Software as a Service implementation, the pricing is per month, with a 6 month minimum implementation. We are offering NASPO/Valuepoint participating entities a 50% discount off of our list price for Software as a Service and a 10% discount on additional hourly services that are requested.

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

In a typical Quest Technology Management/Pondera FDaaS Cloud Software as a Service project, there are no hard costs associated with the implementation of our solution. We note here the anticipated time commitment from various staff members for implementation:

- IT Staff will be required to provide us data extracts on a monthly basis
- IT staff will need to establish site-to-site VPN to the Quest Technology Management/Pondera Cloud
- Program manager will need to approve/authorize users of the SaaS solution

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

FDaaS is a Software as a Service (SaaS) solution. It is a web browser based application and supports any platform that can run Internet Explorer, Chrome, Firefox or Safari. The application is hosted in Quest Technology Management's secure data center. The application resides in a private virtual Local Area Network (vLAN) unique to each client and accessed only through a Lan to Lan Virtual Private

Network (L2L – VPN) or on-demand VPN. FDaaS does not provide an open interface to the Internet. All computing platform requirements are assessed during the requirement phase of the project and based on client data size. These requirements are provisioned at the start of the project and follow a 3 year projected growth pattern. All application and platform provisioning administration is performed by Quest Technology Management/Pondera. Quest Technology Management/Pondera continuously monitors data size and performance and re-adjusts computing platform size and power as needed.

6.6 Scope and Variety of Cloud Solutions

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

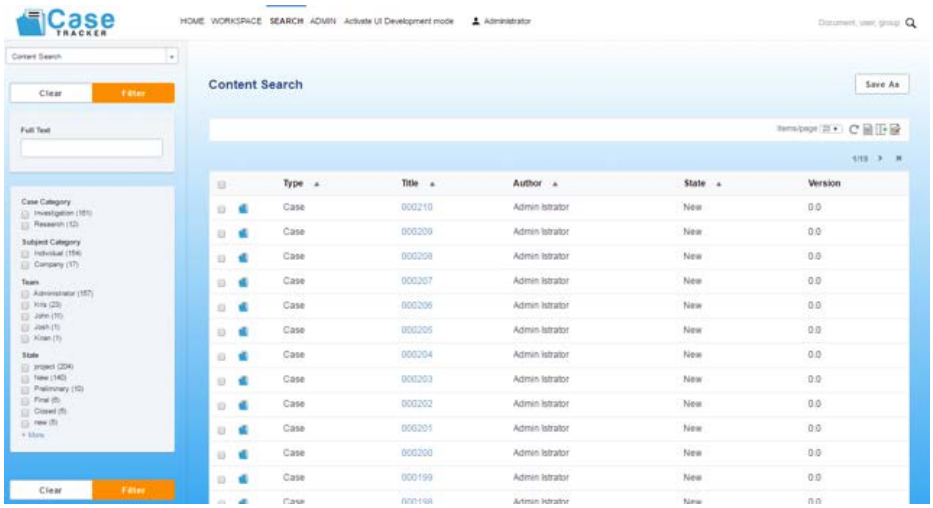
Quest Technology Management/Pondera provides cloud based Software as a Service Data Analytics solutions. The solution includes our Fraud Detection as a Service (FDaaS), with additional modules that include, but are not limited to, Case Management, Network Analysis, Social Media Analysis, and Executive Dashboard.

The **Fraud Detection as a Service** (FDaaS) solution is the primary offering for this proposal. FDaaS is a modern analytics solution designed to detect potential fraud, waste, and abuse in government programs.

FDaaS is a powerful data analytics solution that detects potential fraud, waste, and abuse.

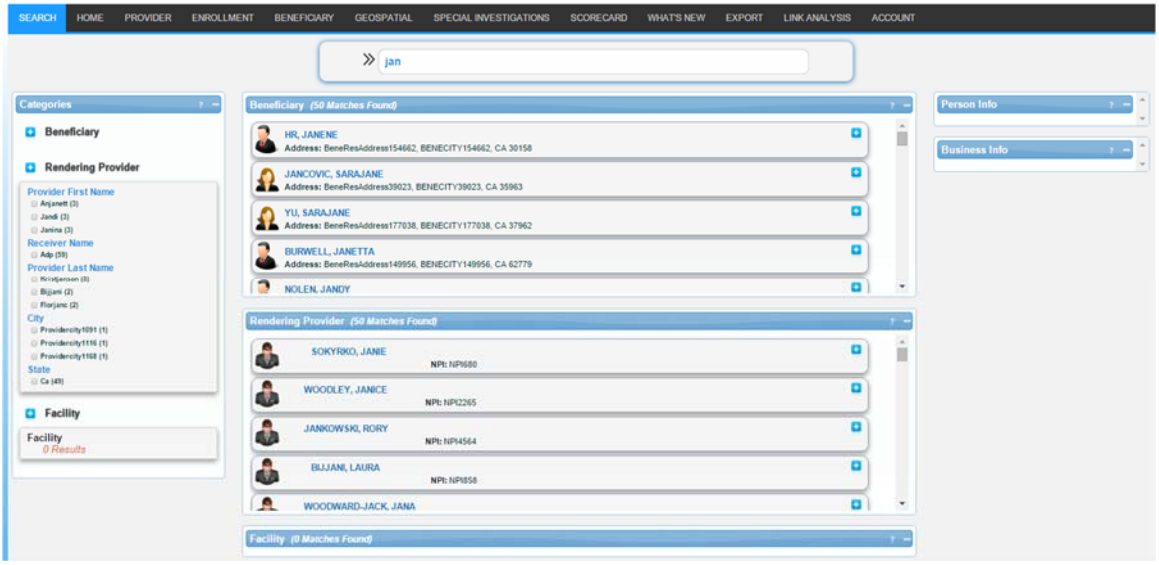
In addition, Quest/Pondera are offering modules that can be added to the base solution.

Case Tracker is a fully-integrated investigative case tracking and management system. Case Tracker imports cases from FDaaS or other sources and uses workflow and rules engines to allow clients to assign and route cases throughout their resolution process.



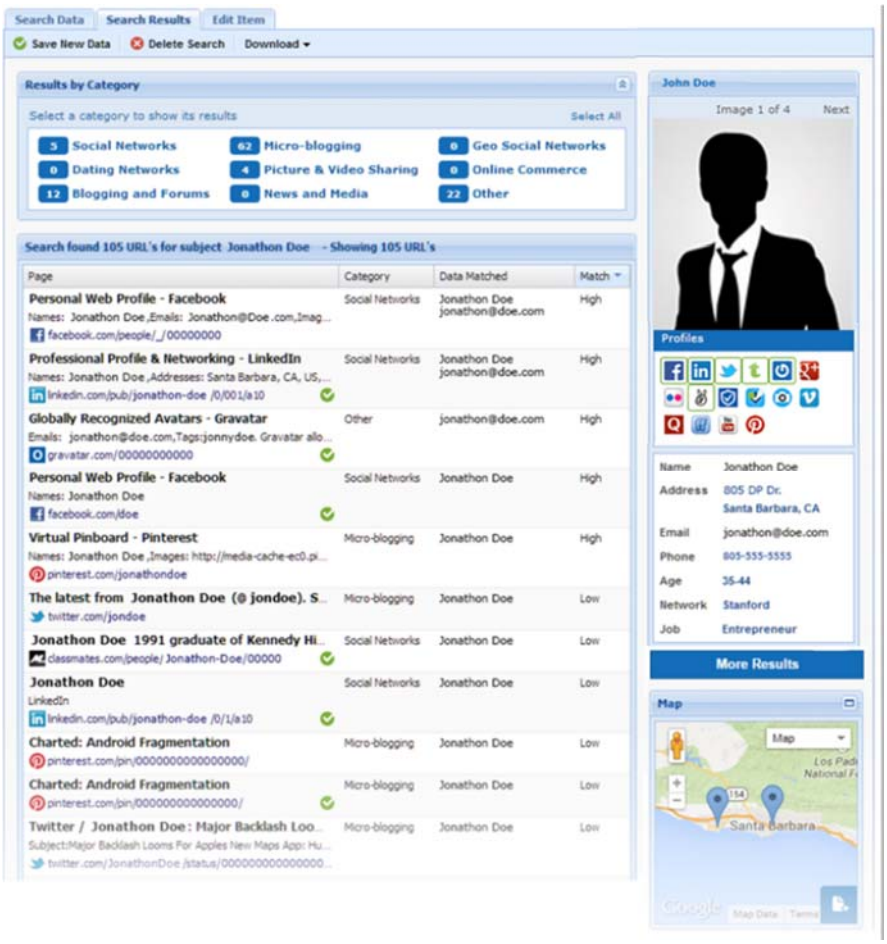
Case Tracker fully integrates case management with the FDaaS solution.

Super Search is an additional module that allows investigators to type in a name or other word and search for matches in the FDaaS database and integrated third-party public records databases. This important investigative tool helps to quickly gather information on suspects who are currently in the program as well as those who are not.



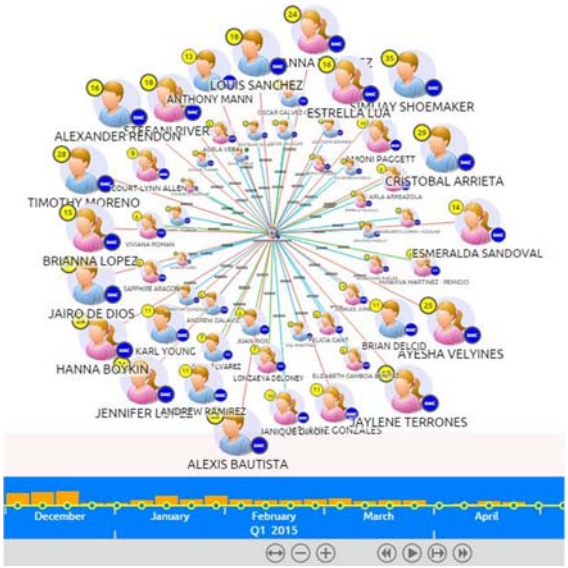
Super Search combs through all database information as well as multiple integrated third party public records databases for comprehensive analysis.

Social Media Analyzer may also be added. Social Media Analyzer combs through social media sites such as social networking sites, blog posts, or other Internet sources where suspects may have left a digital footprint. This allows analysts and investigators to uncover previously unknown connections and activities, such as illicit sales of government benefits. Analysts also use Social Media Analyzer to form a more complete picture of a suspect's relationships, behaviors, and activities.



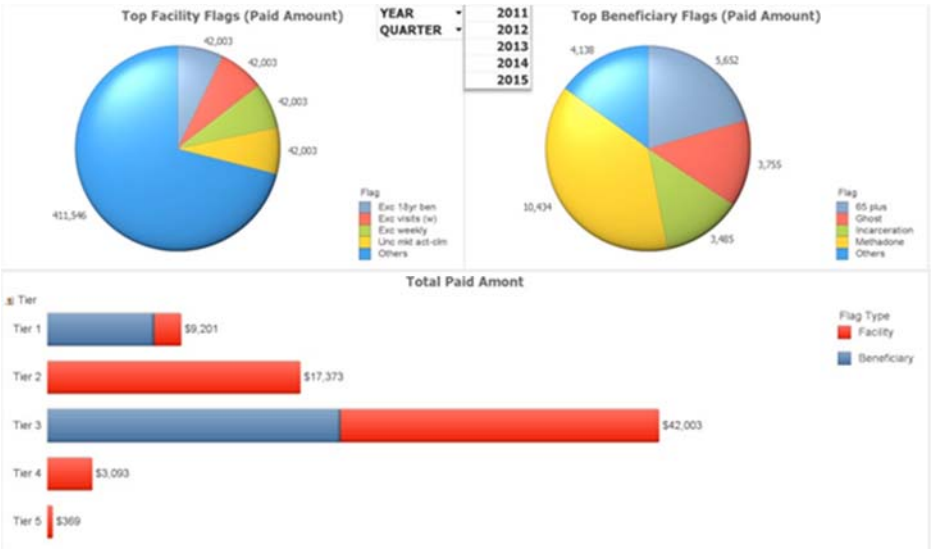
Social Media Analyzer pulls data from multiple social sites to improve knowledge about suspects and their activities and connections.

Network Analyzer is a powerful visualization tool that allows investigators to explore and visualize relationships between and among program providers and beneficiaries. Network Analyzer is fully integrated with FDaaS and allows investigators to examine relationships such as shared program participants or unusual travel patterns.



Network Analyzer can show previously unnoticed connections between program entities over time.

Finally, the **Executive Dashboard** is an intuitive executive reporting system that displays results of the Pondera analytics to program and agency managers. Dashboard users can drill through charts and table sot view changes over time, top flag violations, and other important program information. This helps management to allocate program integrity resources and view the results of their enforcement actions.



The most egregious program violations are highlighted in this Executive Dashboard chart.

6.7 Best Practices

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

Quest Technology Management hosts FDaaS and its infrastructure. Quest Technology Management certifies that its environment is compliant with all security and privacy requirements for each and every FDaaS client organization. Quest Technology Management maintains a comprehensive list of administrative, technical and physical policies and procedures which closely follow the National Institute for Standards and Technology (NIST) and it is SSAE 16 SOC 1 type II certified. FDaaS does not have a direct interface with the Internet. Instead, all users access Quest's secure data center through a LAN 2 LAN VPN connection or on-demand VPN. Each client resides in a unique and separate virtual LAN (vLAN) monitored by an intrusion detection System (IDS). Once the VPN between Quest's secure data center and the client's private network is operational, end users utilize a web browser with secure HTTP (HTTPS) to access FDaaS. All client's data reside on encrypted data store utilizing AES 256 bit algorithm. FDaaS access authorization utilize Role Base Access Control (RBAC). FDaaS employs a verbose access audit trail that can ensure clients only authorized individual gain access to the software.

Organization Profile

7.1 Contract Managers

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

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

Quest's Contract Manager is Ryan O'Keeffe. Ryan is the Director of Service Management. He can be reached from 8 a.m. to 5 p.m. PST at 916.338.7070. His email address is Ryan_Okeeffe@questsys.com

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.***

Ryan O'Keeffe has been with Quest since 2008 and has years of experience with vendor contract negotiations and management. Quest manages Quest's Authorized Reseller agreements with manufacturers' NASPO ValuePoint contracts such as Cisco Systems, EMC, and Palo Alto Networks. In addition, Quest maintains a dozen CMAS (California Multiple Awards Schedules) for various vendors and professional services. As per contract requirements, Quest maintains sales reporting records, fee payments, marketing plan development, and fulfillment specifications. Quest is also on the California IT MSA contract for professional services with multiple professional services designations.

Ryan's resume is attached as Resume-Ryan O'Keeffe RFP.pdf.

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.***

The roles and responsibilities for Ryan O'Keeffe, Contract Manager, as it relates to the NASPO ValuePoint Master Agreement would be to maintain contract requirements as it relates to reporting sales in a timely and accurate manner, tracking and payment of required fees, coordinating Participating Addenda with

State Contracting departments, managing resellers and associated agreements as applicable, and developing and fulfilling marketing plan objectives.

Technical Response

SECTION A: - Complete Narrative of the Offerors Assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements.

FDaaS is a Software as a Service solution provided by Pondera and hosted in Quest's cloud.

Quest will manage the back end of all VM infrastructure and servers including patching of operating systems, anti-virus, application monitoring, patching, backups, VM level High Availability failover, Hot-Site (where required), network, Offeror's side of the Site-to-Site VPN power and physical security.

Pondera will manage everything between Quest and the Purchasing Entity including data cleansing, ETL (Extract, Transform, Load), application configuration, application hosting, application testing, application enhancements, application deployments, software-level redundancy, Purchasing Entity support (Passwords, User Accounts, Roles, etc).

Resources needed to fulfill the requirements on the Purchasing Entity side consist of the following.

- Time of the ISO (Information Security Officer) to enable Quest and Pondera to intake data which may include setting up a System Security Plan and a Data Use Agreement.
- Time of the Network Infrastructure staff to set up and maintaiN
- Time of the database staff and/or vendor to perform one-time and ongoing source data extraction

SECTION B:

8.1 Technical Requirements

We affirm our understanding of, and willingness to comply with, the requirements of Attachments C&D.

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.*

The Quest Pondera team intends to provide Eligible Users with a Software as a Service (SaaS) cloud service model. FDaaS is a Software as a Service private cloud service with the ability to store and secure the purchasing entity's data in the low and moderate FIPS 199 risk categories.

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

8.1.2.1 ***NIST Characteristic – On Demand Self Service: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met.***

FDaaS runs over network and computing architecture that is available 7 X 24 X 365. Clients are able to utilize FDaaS in accordance with their business schedule.

8.1.2.2 ***NIST Characteristic – Broad Network Access: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NSIT Characteristic. Attest capability and briefly describe how network access is provided.***

FDaaS is a web browser based application that supports Internet Explorer, Chrome, Firefox and Safari web browsers. End users access FDaaS from multitude devices that support any of these web browsers over a secure VPN network.

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.***

FDaaS utilizes multi-tenant network and computing infrastructure in a high availability cluster with a private virtual resources uniquely allocated to each client.

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.***

Quest Technology Management continuously monitors the usage of the network, storage and computing resource pools and adjusts them as required to maintain continuous operation. Quest Technology Management/Pondera does not include computing infrastructure utilization in its client pricing model.

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.***

Quest can report on and adjust resources available to end users at any time. FDaaS has an extensive audit trail that allows administrators to determine how many and who are the users utilizing the software.

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.***

Quest Technology Management/Pondera offers a single Software as a Service (SaaS) solution. Our primary service category is SaaS Analytics: Data Analytics offerings.

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

Quest and Pondera are willing to comply with the requirements of Attachments C and D.

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.***

Pondera is committed to supporting FDaaS as a SaaS with low and moderate levels of FIPS 199 data criticality levels. The Quest hosted solution will meet and exceed the expectations put forth in Attachment D.

Quest's offerings adhere to the services, definitions and deployment models identified in the Scope of Services for cloud services and are compliant with NIST Special Publication 800-145 practices as it relates to the categorization of risk, and

the five essential NIST characteristics, three service models and four deployment models.

Quest-Pondera provides the 5 Essential Characteristics:

On-demand self service

- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Quest-Pondera offers the 3 cloud-based service models

- SaaS
- IaaS
- PaaS

Quest-Pondera's cloud-based services are available through the following 4 deployment methods:

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

8.2 Subcontractors

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 na 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.***

Quest is teaming with our subcontractor, Pondera Solutions, to provide cloud based Software as a Service Data Analytics for fraud detection services. Quest and Pondera have been partners since February 2015. Together, we have delivered cloud based data analytics for fraud detection to multiple government agencies around the country including the California Department of Health Care Services,

California Employment Development Department, and both the Iowa Workforce Development Division and Department of Public Health.

The Quest – Pondera partnership is a logical one. Pondera offers their solution, Fraud Detection as a Service (FDaaS), and Quest Technology Management hosts the solution and provides security and additional functions such as product penetration testing. By separating the data hosting and security from the product development of the detection system, we provide additional checks and balances.

Our partnership arrangement also allows both companies to focus on what they do best: Quest on system hosting and security, Pondera on delivering innovative fraud detection solutions. This results in a modern, secure, system which can be deployed rapidly (typically in less than 90 days) and can scale to meet the requirements of the largest programs in state government.

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.***

Pondera Solutions will provide the detection system, Fraud Detection as a Service. This system will be housed within the Quest Datacenters. In addition, Pondera will fill the following positions:

- Project Manager – The Quest/Pondera Project Manager will coordinate the timely delivery of implementation and services. They will coordinate meetings with Quest and the Participating Entities to ensure solution delivery is timely and satisfactory.
- Special Investigations support – An integral part of the Pondera FDaaS solution is Special Investigations support for clients. The investigative support team helps with deep dive investigations to help augment case development for clients.
- Subject Matter Experts – Pondera provides subject matter experts to help translate each program's goals into deliverables in the FDaaS dashboard.

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.***

Pondera Solutions is the leading provider of cloud-based data analytics and fraud detection services for government agencies. Pondera's core system, Fraud Detection as a Service (FDaaS) uses data matching services, procedural rules, and prediction models to detect and help prevent fraud. In production since 2012, it is currently helping government agencies identify, prevent, and collect hundreds of millions of dollars annually.

FDaaS is currently available for Medicaid, Unemployment Insurance, Revenue Tax, Social Services, Integrated Eligibility, and Welfare programs. It has been deployed or is in the process of being deployed to 16 programs in 6 states. This includes several of the country's largest state-administered programs including the California Medicaid and Unemployment Insurance Programs.

Pondera and FDaaS have received a number of awards. The Sacramento Regional Technology Alliance (SARTA) named Pondera the Next Tech Innovator of the Year in 2014. Government Technology named Pondera to the 2016 GovTech 100 list of companies making a difference in the state and local government technology market. And Google has invited Pondera to speak at two of their annual Innovation of the Nation events.

Quest will ensure that Pondera and Pondera employees meet all Statement of Work Requirements.

8.3 Working with Purchasing Entities

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.*

Quest utilizes a variety of reports to monitor security and network activity and identify potential problems, including daily incident reports, which are managed following a documented incident response process. This process establishes roles, responsibilities, and communications procedures for handling computer security incidents by the Quest Security Incident Response Team.

- The personnel involved begins with the Quest IT staff at the Network Operations Center who identify and report the incident to Pondera Solutions. Quest staff will work with the Pondera Solutions support staff as necessary to isolate, notify, and/or recover from any identified security incidents. The Quest/Pondera team will coordinate through the Contract Manager identified in Section 7 to communicate with the point of contact for the Purchasing Entities via email and/or phone with status updates throughout the remediation process.
- Quest response times are established in the Service Level Agreement with Pondera Solutions. Communications with the Purchasing Entities will be in accordance with this agreement.
- Processes and timelines are dependent on the Service Level Agreement and the agreed upon Security plan with the Purchasing Entities. Incidents are assigned a level of criticality between 1 and 5 with 5 being the most critical.
- Methods of communication and Quest assistance are dependent on the Service Level Agreement, though generally communication would be via email or phone.
- Other information to augment the understanding of our Service Offering is that Quest Managed Services is responsible for managing the Pondera Solutions' computing infrastructure for all existing clients as well as any new clients. As part of their ongoing responsibilities, Quest Managed Services staff performs the following:
    - Utilize security monitoring tools to identify security incidents on client networks, systems, and/or applications
    - Provide incident analysis
    - Notify clients of security incidents
    - Create security related reports
    - Review and recommend security improvement measures on an ongoing basis

Quest structured its Federal Security Operations Center (SOC) as a multi-layered capability providing thought leadership for industry regulations, e.g. NIST, DFARs, and NASA FARs. In addition to Federal capability, Quest also provides SOC services for Financial and Healthcare customers. By partnering with Quest, purchasing entities will benefit from this because as your trusted partner, we look across multiple industries to better understand Advanced Persistent Threats.

Quest's Federal SOC would work with purchasing entities to introduce a highly integrated solution that consolidates inbound and outbound internet traffic to key redundant locations that are GEO load balanced by leveraging Quest Cloud services.

Quest will introduce a multi-tiered SOC managed services capability to meet the requirements of the purchasing entities' compliance business:

Log Retention	We can use a SIEM that will collect, archive, search and report raw data from company devices, network infrastructure, servers and mobile devices.
Log Monitoring	24x7 real-time analysis of logs and alerts
Firewall and VPN Management	Full lifecycle management monitored 24x7
Web Security Service	URL filtering, Web Content Filtering and policy enforcement
Risk mitigation and consulting	Provide thought leadership to help purchasing entities understand and implement compliance requirements and perform and mitigate risk analysis outcomes
Managed IDS/IPS	Full lifecycle management monitored 24x7
Advanced Persistent Threat Services	Data correlation from all Quest SOC environments to produce actionable data on Advanced Persistent Threats
Vulnerability Management	Both internal and external vulnerability scanning management
Penetration Testing	Proactive testing evaluating the security of existing systems
Web Application and Security services	Web scanning to identify and mitigate security risks

Quest's Federal SOC services will also work with purchasing entities to introduce additional controls as needed upon completion of a Risk Analysis:

Quest will work with client's business units to understand company gaps, risk and priority to quickly mitigate existing threats. Quest Federal SOC has canned templates, security configuration and capability allowing clients to customize as needed.
Access Control: Account management, enforcement, wireless security, mobile device management, etc.
Awareness & Training: User training, etc.
Auditing:

Event audit, content and records analysis and reporting, time stamping, etc.
Configuration Management: Baseline configuration and setting, least functionality, information system component inventory, etc.
Contingency Planning: Information system backup, etc.
Identification & Authentication: Identifier and authenticator management, password management, etc.
Incident Response: Incident response training, handling, monitoring and reporting, etc.
Maintenance: Non-local maintenance, crypto, personnel, etc.
Media Protection: Media storage, sanitization, etc.
Physical & Environment Protection: Physical access authorizations, access control, control for output devices
Risk Assessment: Vulnerability scanning
System & Communications Protection: Application partitioning, information in shared resources, boundary protection, transmission confidentiality and integrity, crypto, etc.
Systems & Information Integrity: Flaw remediation, malicious code protection, system monitoring
Program Management: Security authorization process

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.***

The Quest Pondera team 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.

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

In addition to a FDaaS Production environment, a User Acceptance Test, or UAT environment is hosted. The UAT environment is identical to the Production environment in terms of hardware, software, data and application settings. This environment is used to ensure mandatory requirements; functionality or performance measures are met prior to a Production push.

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.***

FDaaS does support and will be configured to support applicable accessibility standards established under section 508 of the Rehabilitation Act. The Quest Pondera Team will comply with Participating entity accessibility policies and the Americans with Disability Act, as applicable.

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

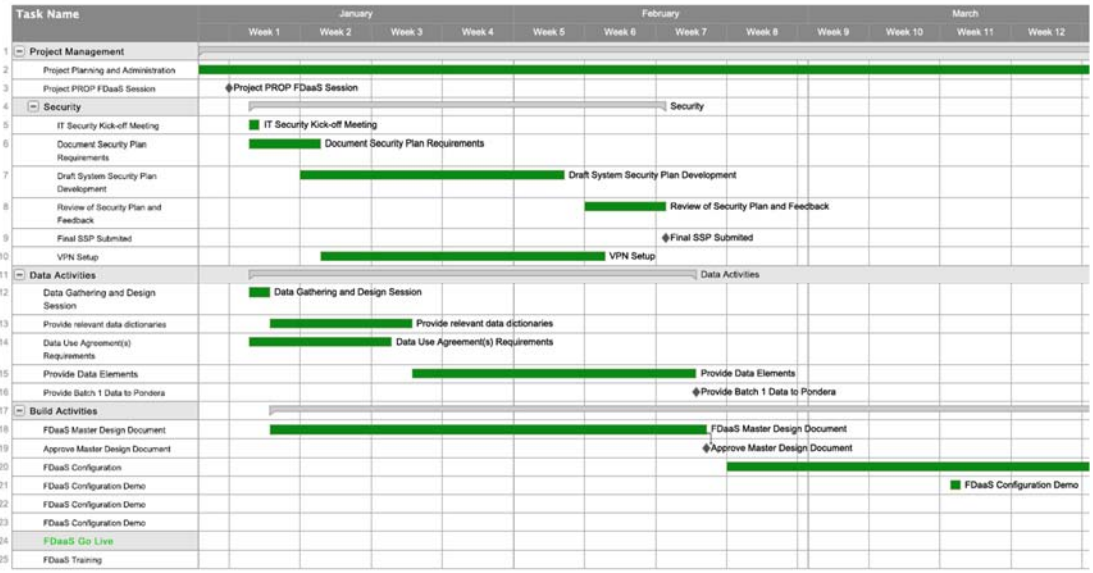
FDaaS fully supports all modern browsers that have HTML5 and JavaScript support including the newest versions of IE, Firefox, Chrome, and Safari

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.***

The Quest/Pondera team will meet with the Purchasing Entity and cooperate 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. All of our implementations include PII and PHI, whether for health, welfare programs, tax systems, or other government programs. We are very well versed on the rules and regulations surrounding sensitive data storage and usage and we take security extremely seriously in terms of how we store and process data.

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 Quest/Pondera team utilizes task oriented project management to ensure proper workflow and progress benchmarking. A Sample Project Plan is shown below:



We anticipate 90 days for implementation from the receipt of data. Prior to receipt of data, a Security Plan must be agreed upon in order to ensure the safe transmission of sensitive data.

8.4 Customer Service

8.4.1 *Offeror must describe how it ensures 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).*

Quest and Pondera are committed to ensuring excellent customer service to Purchasing Entities. We anticipate utilizing Quality Assurance measures, Escalation plans, and our Service Level Agreements to ensure the highest quality of customer service.

- **Quality Assurance Measures**

In order to deliver a high-quality solution and analytics output from this solution, a number of different tests are conducted including the following:

- Analytics Output Validation/Quality Assurance
- Smoke Test
- Unit Test
- Impact Analysis Test
- User Acceptance Testing (UAT)

With every new design build, the Pondera team conducts internal testing on the new report or functionality in a designated Purchasing Entity development and staging environment. Once internal testing is complete, Pondera will deploy the new report or functionality to the Purchasing Entity for their user acceptance testing.

Objectives	Expected benefits
▪ Create test environment based on finalized configuration ▪ Create and finalize test scripts ▪ Execute smoke, unit, and impact analysis testing ▪ Complete user acceptance testing (UAT) and report results	▪ Delivers a thoroughly tested business process and application ▪ Provides operations team members with requisite knowledge of the solution to provide effective support

Key activities	Key deliverables
▪ Perform Analytics Output Validation/Quality Assurance ▪ Perform Smoke Test ▪ Perform Unit Test ▪ Perform Impact Analysis Test ▪ Perform User Acceptance Testing	▪ Completed Test Scripts ▪ Test Metrics ▪ User acceptance testing (UAT) acceptance plan and sign-off

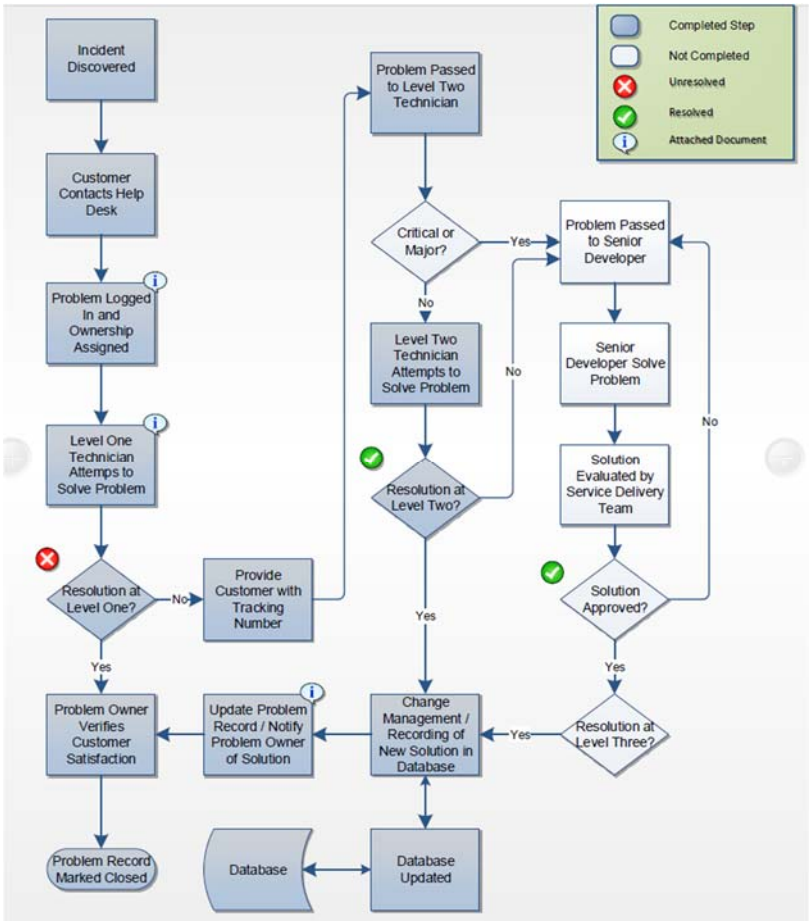
Test step detailed activities

Key activity	Description
Perform Analytics Output Validation/Quality Assurance	The Pondera Special Investigations Unit (SIU) will conduct tests on analytic results for all the following elements in the solution dashboard: • Reports • Profiles • Geospatial Analytics • Scorecards • Network Analysis tool • Export Function • Executive Information System The quality of the FDaaS analytics is a key differentiator of the Pondera solution and is built into the process from start to finish. Ingesting large data sets from the Participating Entity and third-party sources and pushing substantial volumes of data to users without any "real world" validation can result in a deluge of alerts without any meaningful priority or triage process and false positives that waste precious investigative time and resources. To avoid this, the Pondera SIU will independently review and validate third-party data to ensure that the source data is only cross-matched to relevant and valid outside data sources. Then the output of the flags, geospatial analysis, scorecards, etc. will be reviewed with the Participating Entity prior to production deployment to ensure that the final delivery meets expectations.
Perform Smoke Test	Pondera will perform a Smoke Test on the following elements for the core Participating Entity deployment, as well as each subsequent module deployment, prior to go-live: • Test login • Test audit logging • Test Overall core system functionality • Test interactions with integrated components • Test logout We will utilize standard test plans/scripts to ensure the system is functioning normally. These standard test plans/scripts are living documents that are added to each time we add or change system functionality.

Key activity	Description
Perform Unit Test	The purpose of unit testing is to verify that the development and system components are functioning as expected and to confirm that no errors exist. Unit testing is performed during the configuration and development efforts. The unit test will be executed leveraging our unit testing scripts and is intended to verify that the specific design or configuration is working as expected prior to further testing.
Perform Impact Analysis Test	Impact analysis testing will validate the system is operational and performs without errors in an end-to-end test cycle. We will perform the following Impact Analysis process: Review from a technical/code/database level for any possible problems that could have been caused in non-related FDaaS components Review from a business/functionality level for any possible problems that could have been caused in non-related FDaaS functions. The functional team performs impact analysis testing to determine whether or not the new feature has impacted any pre-existing functionality.
Perform User Acceptance Testing	The objective of User Acceptance Testing (UAT) phase is to demonstrate the application's ability to meet the Participating Entity's requirements. The end-users perform acceptance testing to accept FDaaS functionality relative to the agreed upon requirements and design specifications. A formal acceptance plan including entry and exit criteria will be created and agreed upon by the Participating Entity and the Pondera team. The UAT acceptance plan leverages scenarios and scripts already executed in the impact analysis test step. This set of scenarios and scripts are identified and selected by the Participating Entity to validate acceptance of the solution. Participating Entity personnel shall execute, with assistance from the Pondera Team, the user acceptance testing scripts as defined in the acceptance plan. The purpose of the acceptance testing phase is to provide validation of functions deemed mandatory for acceptance of the production solution. This testing phase will require signoff by the Participating Entity to provide formal acceptance of the Participating Entity solution prior to go-live.

- **Escalation plan for addressing problems and/or complaints**

Pondera has a straightforward escalation process designed to rapidly address any client issues. As a Software as a Service (SaaS) application, we expect to maintain a queue of system enhancements. In addition, all software contains bugs. While we deliver high quality software, we also recognize the need for stringent issue logging and resolution processes.



The Pondera issue tracking and resolution process is followed regardless of the channel used to log the issue.

Pondera's engagements tend to be very cooperative in that our virtual Special Investigations Unit (SIU) becomes embedded within the Purchasing Entity's program integrity team. This allows us to recognize and correct issues early, drastically reducing the need to escalate issues. However, if there are software or project issues that are not met to the satisfaction of the Purchasing Entity, they will be able to escalate issues through the following process.

- **SIU Representative**: The designated SIU representative is the first contact for project issues. The SIU representative is responsible for monitoring system use, tracking bugs and enhancement requests, validating, formatting, and delivering reports, and leveraging additional Pondera staff.
- **Quality Assurance Managers**: If the SIU representative is not meeting expectations on an issue(s), requests can be escalated to Amanda Huston or Tom Lucero, the functional and technical QA managers. As members of the Pondera executive team, Amanda and Tom have the staff and approval authority to quickly solve the large majority of customer issues.
- **Chief Operating Officer**: In the unlikely event that the Quality Assurance Managers fail to resolve the issues, the next level of escalation is to Greg Loos, Pondera's Chief Operating Officer. Greg manages Pondera's Human Resources and Financial Management team and has the authority to support and approve actions requested by Amanda and Tom. Greg has the ability to bind the company and direct any and all company resources to solve client issues.
- **Chief Executive Officer**: Jon Coss, Pondera's CEO, is the final level of escalation. Jon also serves as an active participant on major project steering committees, including Participating Entity committees if desired. Jon has authority to bind the company and direct company resources to solve issues.
    - Service Level Agreement (SLA)
      Our Service Level Agreement is attached at the end of this response.

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

a. ***Lead representative for each entity that executes a Participating addendum.***

Amanda Huston, VP of Service Delivery, will be the Lead Representative for each entity that executes a Participating Addendum.

b. ***Customer Service Representative must be available from 7 a.m to 6 p.m. Monday through Sunday for the Applicable Time Zones***

We will provide dedicated Customer Service Representatives who will be available from 7 a.m. to 6 p.m. Monday through Sunday for all Applicable Time Zones.

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

Our Customer Service Representatives will respond to inquiries within one business day.

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

Any design services would already be included as a part of the custom configuration for each Cloud Software as a Service Data Analytics implementation.

e. ***You must provide installation Services for the applicable categories*.**

There is no installation service as this is a Cloud software implementation.

8.5 Security of Information

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.*

An engagement of this nature requires significant considerations to the management of data requiring strict levels of security. In dealing with government and healthcare clients throughout the world, we understand and are committed to the proper handling of sensitive data. The security management plan addresses the adequate security of each major application by taking into consideration the security of all systems in which our application will operates.

Security Planning: system security planning process starts with identifying the project risks related to non-compliance and the risk of data breach.

Security Development: system security development includes security requirements that are outlined in the Cloud Solutions Requirements. There are three types of safeguards:

Administrative: relate to the documented policies and procedures related to day-to-day activities and operations.

Physical: adopted measures for protecting the Department’s information systems and confidential information from environmental hazards and unauthorized intrusion.

Technical: adopted security measures for using technology to protect the data gathering, storing, and transmitting between the Participating Entity and the Quest Pondera team.

Pondera has strict administrative, technical, and physical controls in place to protect clients' data. The facility is hosted by Quest Technology Management and is ANSI TIA-942 tier 3 data center or higher for architectural, electrical, and mechanical requirements. Physical access to the infrastructure is controlled by multiple layers of access controls including proximity card access, biometrics, and physical cages. The client's data is stored on an AES 256 bit encrypted data store. Each client's infrastructure is isolated to a unique dedicated private vLAN, dedicated virtual infrastructure and monitored by an IDS system. The infrastructure is built upon a high availability architectural configuration using a VMware hosts and a central redundant Storage Area Network (SAN). FDaaS does not have an interface with the open Internet. Clients access FDaaS through a Lan 2 Lan VPN (L2L-VPN through IPSec) and a web browser over secure HTTP (HTTPS channel). This creates a dual secure channels at both the application and network layers. Client's native data is transported to the FDaaS data stores via secure FTP (sFTP) over the encrypted L2L-VPN which also creates dual secure channels at both the application and network layers. Data backups and/or snapshots and frequency are available based on data owner's requirements. At the conclusion of the contract or based on client's data retention/disposal requirements, Quest/Pondera would ensure data is appropriately destroyed. Data destruction is specific to the storage requirements of the client and can take one of the following forms:

- Disposal of the encryption keys.
- Force overwrite of the area on disk in which data resides.
- Physical destruction of storage media including but not limited to shredding.

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

Pondera closely follows the National Institute for Standards and Technology (NIST) 800-53 security controls for the Federal Information Processing Standard (FIPS) 199 criticality level defined by our clients to protect their Personally Identifiable Information (PII), electronic Protected Health Information (ePHI under HIPAA) and Federal Tax Information (FTI under IRS 1075) data. Other applicable laws relevant to Pondera and FDaaS are:

- The Privacy Act of 1974
- Computer Security Act of 1987
- Paperwork Reduction Act of 1995
- Clinger-Cohen Act, Information Technology Management Reform Act of 1996
- Presidential Decision Directive 63 (PDD63), May 1998
- OMB Circular A-130
- Homeland Security Act of 2002
- Sarbanes-Oxley Act of 2002
- E-Government Act of 2002
- Federal Information Security Management Act (FISMA) of 2002
- Homeland Security Presidential Directive – 7, December 2003
- Homeland Security Presidential Directive – 12, August 2004

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.***

Pondera has strict access controls to prevent unauthorized access to clients' data other than under very specific conditions. Access to the client's environment is driven by Role Based Access Control (RBAC). For authorized individuals with access to these environment, access is permitted only as a result of configuration/change management process agreed with clients. The FDaaS environment has a robust access audit trail allowing both Pondera and clients to determine the necessary access review requirements.

8.6 Privacy and Security

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

At Quest's data center, there is a range of network security capabilities in place such as intrusion detection, the ability to monitor line for traffic and capabilities for Managed Distributed Denial-of-Service attack (DDoS) prevention. Firewalls are in place at all externally facing access points to control access to all network and security platforms. Firewall activity is monitored on a daily basis through the use of

reports generated from various systems. Quest utilizes many tools and techniques to secure infrastructure.

Regulatory Compliance: NIST 800-53/FEDRAMP/ITAR

Quest maintains the following applicable certifications:

- Cisco Advanced Data Center Architecture Specialized Partner
- Cisco Master Service Provider Certification for cloud and managed services.
- Cisco Advanced Content Security Specialization
- Microsoft partnership with on-prem. Azure presence
- Engineers with top security, ISAC
- CISSP, CISSO, CRISC, SAN, CCIE
- Several Quest Data Center team members hold ITIL/ITSM certifications
- SOC Type II report

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.***

We currently hold the following designations:

- NISPOM
- DoD 5220.22-MHIPAA Compliant

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*****.**

The Quest data center provides a Security Management function that protects information assets against risks and ensures their confidentiality, integrity and availability. Security is handled in a hosted environment in a very similar manner to how it is supported in a Client hosted model. Identity and access management will continue to be undertaken by Client staff and the system will need to conform to Client security standards and integrate into Client security and identity and access management infrastructure.

Quest provides periodic and on-demand system upgrades and patches. Servers are monitored regularly for updates, utilizing the same tools that are used to monitor client patch requirements. Servers are updated with patches as identified. Quest

also subscribes to many vendor notification services to maintain awareness of these issues.

Quest provides a regular assessment of vulnerabilities for the information systems in the environment. Security engineers perform monthly vulnerability tests. An outside security firm executes annual internal vulnerability assessments. An executive summary with test and assessment results is available by request to validate the execution of these processes.

Quest provides regular penetration testing and reports. An outside security firm executes annual external penetration tests. An executive summary with test and assessment results is available by request to validate the execution of these processes.

Quest provides regular application and system security testing.

Quest will provide standard monthly, quarterly and annual security reports that describe security related activities undertaken.

Quest-Pondera follows a documented access control policy that covers network access as well as physical facility access and perimeter security.

Network Access Control: Every router, switch, or firewall capable of being configured to utilize ACS (Access Control System) must be configured to do so and adhere to the following guidelines:

- Routers must use TACACS+ for all user authentications. In the event of a TACACS+ failure, local accounts are used.
- ACS log data will be archived for one year.
- Weekly review of log data and validate any changes followed defined change management policy.
- The enable password on the device must be kept in a secure encrypted form.
- Disallow web services running on devices where not required for device management.
- Use corporate standardized SNMP community strings.
- Access rules are to be added as business needs arise.
- Device must be included in the corporate enterprise management system with a designated point of contact.

Physical Access:

Access to Quest's Service Delivery Center is strictly monitored and requires badged entry. Access to the Service Delivery Center is based on need and at the sole discretion of Quest. Requests for access must be approved by an authorized representative of each entity who is registered with Quest Operations as an authorized entity approver.

- Visitors are not allowed in the data center without approval.
- Visitor access to the data center is at the discretion of Quest.
- Approved Visitors must obtain a Visitor's badge before entry into the Quest facility while in the presence of the Visitor's approved Sponsor.
- Approved Visitors must be escorted by an approved Sponsor at all times.
- Sponsors are responsible for ensuring approved Visitors follow all Quest data center rules and guidelines.
- Upon completion of the visit, the Visitor is responsible for returning the Visitor badge to Quest Operations. Personal ID cards surrendered during the visit will only be returned to the respective Visitor.

Quest will introduce a multi-tiered SOC managed services capability to meet the requirements of the purchasing entities' compliance business:

Log Retention	We can use a SIEM that will collect, archive, search and report raw data from company devices, network infrastructure, servers and mobile devices.
Log Monitoring	24x7 real-time analysis of logs and alerts
Firewall and VPN Management	Full lifecycle management monitored 24x7
Web Security Service	URL filtering, Web Content Filtering and policy enforcement
Risk mitigation and consulting	Provide thought leadership to help purchasing entities understand and implement compliance requirements and perform and mitigate risk analysis outcomes
Managed IDS/IPS	Full lifecycle management monitored 24x7
Advanced Persistent Threat Services	Data correlation from all Quest SOC environments to produce actionable data on Advanced Persistent Threats
Vulnerability Management	Both internal and external vulnerability scanning management
Penetration Testing	Proactive testing evaluating the security of existing systems

Web Application and Security services	Web scanning to identify and mitigate security risks

Quest's Federal SOC services will also work with purchasing entities to introduce additional controls as needed upon completion of a Risk Analysis:

Quest will work with client's business units to understand company gaps, risk and priority to quickly mitigate existing threats. Quest Federal SOC has canned templates, security configuration and capability allowing clients to customize as needed.
Access Control: Account management, enforcement, wireless security, mobile device management, etc.
Awareness & Training: User training, etc.
Auditing: Event audit, content and records analysis and reporting, time stamping, etc.
Configuration Management: Baseline configuration and setting, least functionality, information system component inventory, etc.
Contingency Planning: Information system backup, etc.
Identification & Authentication: Identifier and authenticator management, password management, etc.
Incident Response: Incident response training, handling, monitoring and reporting, etc.
Maintenance: Non-local maintenance, crypto, personnel, etc.
Media Protection: Media storage, sanitization, etc.
Physical & Environment Protection: Physical access authorizations, access control, control for output devices
Risk Assessment: Vulnerability scanning
System & Communications Protection: Application partitioning, information in shared resources, boundary protection, transmission confidentiality and integrity, crypto, etc.
Systems & Information Integrity: Flaw remediation, malicious code protection, system monitoring
Program Management: Security authorization process

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).***

Quest provides monitors for account provisioning, security systems configuration change and user login and user profile change activities. Quest's processes are documented in the IT Access Policy which covers password policies, System Administration Standards, Employee Access, User Access, User Responsibilities, User Authentication for External Connections, OS/AD access control, Management Application and Information Access, Policy Compliance and Governance. Quest has tools installed to remotely wipe data from mobile devices. Quest employees use securely-accessed, virtual desktops that are centrally managed and monitored.

Quest's data protection services include:

- Encryption
- Automatic elimination of data on stolen or lost equipment
- Remote data destruction
- On Demand Vulnerability
- Assessment reporting
- Data Security Assessments
- Online Backup or Replication

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

Quest is currently SSAE 16 SOC2 Type 1 certified with SOC 2 Type 2 expected to be completed in March 2016. Additionally, Quest maintains certifications with industry-leading manufacturers, such as Cisco Systems, including the following examples:

- Cisco Advanced Data Center Architecture Specialization
- Cisco Advanced Security Architecture Specialization
- Cisco Powered Managed Security
- Cisco Powered Infrastructure as a Service
- Cisco Powered Disaster Recovery as a Service

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.***

Pondera Solutions, Inc. employs logging functions from a web, application, and database level. These functions include but are not limited to, user IDs or other identification mechanism, dates, times, and details of events key to the operation of the IT Resource, Records of successful and rejected system access attempts, Records of successful and rejected access to data and other IT Resources, Changes to IT Resource system configuration, Use of privileged access or operations (to include the use of privileged accounts), Use of system utilities and applications, Files accessed and the kinds of access, source and target network addresses and protocol details, system log exceptions, network management alarms, alarms raised by access control systems), Activation and deactivation of protection systems such as anti-virus, intrusion detection, and file integrity systems.

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

Pondera Solutions, Inc. employs a role based access control (RBAC) policy which bases access control decisions on the functions a user is allowed to perform within a particular role or group. Thus the RBAC policy allows for the restriction of data, functions and /or documents to specific users or groups. It should be noted that users cannot pass access permissions on to other users at their discretion.

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.***

A security incident can originate from various sources; the client, Pondera, or Quest Technology Management. Pondera designates a project/client advocate manager that acts as a Point of Contact (POC) for each engagement. Any security (or suspected security) incidents discovered by our clients are immediately reported to the POC which internally escalates it the Pondera Information Security Officer (ISO). When Pondera or Quest Technology Management detect actual or suspected security incidents, they are immediately reported to Pondera's ISO. The Pondera ISO investigates and validates whether the reported incident is a security

incident. If the scope of the incident includes Quest Technology Management, Pondera has established a strict urgency based Service Level Agreement (SLA) with Quest Technology Management. For severity 1 issue like a security breach, work begins within minutes from the time the incident is identified and/or reported and response could, but not limited to, taking the FDaaS servers offline to ensure data is no longer accessible through the network. The Pondera ISO and the clients designated authorized incident response individuals work closely and establish an action plan which would follow the incident to its resolution. Post security incident, Pondera employs a lessons learned process that is aimed to address any vulnerabilities discovered during the incident resolution process.

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.***

Quest structured its Federal Security Operations Center (SOC) as a multi-layered capability providing thought leadership for industry regulations, e.g. NIST, DFARs, and NASA FARs. In addition to Federal capability, Quest also provides SOC services for Financial and Healthcare customers. By partnering with Quest, purchasing entities will benefit from this because as your trusted partner, we look across multiple industries to better understand Advanced Persistent Threats.

Quest's Federal SOC would work with purchasing entities to introduce a highly integrated solution that consolidates inbound and outbound internet traffic to key redundant locations that are GEO load balanced by leveraging Quest Cloud services

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).***

Quest-Pondera employs a wide range of network, server, and application security capabilities that detect, alert, and block security threats. These can include intrusion detection, the ability to monitor line for traffic and capabilities for Managed Distributed Denial-of-Service attack (DDoS) prevention, SQL injection attacks, malware/virus zero day infections, and correlation of events. Quest utilizes many tools and techniques to secure infrastructure. Security services are dependent on the level of engagement outlined in the client's SLA.

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.***

Offers of employment are extended by managers of the department and are contingent upon successfully passing a criminal history background check, drug-screening for selected positions, verification of previous employment history, and educational credentials.

Personnel receive training on Quest's security program through Inspired Learning's Security Awareness Training. New hires, employees and subcontractors must complete mandatory annual training.

Quest uses various computer logging/monitoring tools for employees. Employee remote access is conducted through a secure VPN access.

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.***

Quest structured its Federal Security Operations Center (SOC) as a multi-layered capability providing thought leadership for industry regulations, e.g. NIST, DFARs, and NASA FARs. In addition to Federal capability, Quest also provides SOC services for Financial and Healthcare customers. By partnering with Quest, purchasing entities will benefit from this because as your trusted partner, we look across multiple industries to better understand Advanced Persistent Threats.

Quest's Federal SOC would work with purchasing entities to introduce a highly integrated solution that consolidates inbound and outbound internet traffic to key redundant locations that are GEO load balanced by leveraging Quest Cloud services.

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.***

Quest has a defined incident management process regarding notification to both the State and Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

<u>Incident and Problem Management</u>

All incidents and alerts are logged, tracked and maintained through a ticketing system. Incidents are entered manually into the system and given a ticket number after a customer calls, emails, or faxes in their problem. The ticketed incident is classified, assigned a severity level and given to the appropriate engineering personnel for resolution. If the incident is unable to be resolved, it is escalated to QMS management for resolution. Recurring incidents and incidents where a workaround was applied are investigated further through the Problem Management analysis team. Detailed components of the work flow process are described in Quest's "Incident Response", "Client Call Process" and "Problem Management" manuals which are part of Quest's on-line documentation available for review at any time by personnel. Quest's internal incident response process consists of the following phases. Once the appropriate preparative steps have been taken, the Incident Response Process consists of a six-phase cycle.

- Preparative
- Prevention
- Identification
- Containment
- Eradicate
- Recovery
- Follow-up

Client Managed Services Incident Response Process:

Internal support of the Incident Response Process at Quest supports the full Incident Response lifecycle. While Quest can support the full Incident Response life cycle for its clients, Quest is rarely engaged to do so. Generally, clients prefer to have Quest provide the monitoring, alerting, and reporting functions, which exist in the prevention, identification, and follow-up tasks of Incident Response. The client is then responsible for containment, eradication, and recovery. Generally the preparation step consists of billable time, which is built into the Managed Services turn-up process.

- Preparation
- Prevention
- Identification
- Follow-up

Preparation

As stated earlier, the most critical facet of incident response is in building the policies and processes that support the management of the security infrastructure. Clients are encouraged to develop documented processes and procedures for security management if they aren't already in place. Quest Professional Services may be engaged to develop such processes and procedures if necessary. Additionally, the client should have a designated Incident Response Team in place that can react to incidents identified and reported by Quest. Preparation accordingly limits the potential for damage by ensuring response actions are known in advance and well coordinated. Quest-Pondera maintains the following objectives for the purchasing entities.

- **Communicate 'Use' policies for systems, applications, and networks**
  'Usage' policies dictate how, when, and by whom client networks, systems, and applications may be used. To effectively monitor a client's environment, Quest must have knowledge of these 'Usage' policies.

- **Post warnings**
  Clients are strongly encouraged to post a banner stating their authority to monitor network and system activities and defend against attacks. Banners are to be placed on all network and system resources that reflect the policies stated for appropriate use of client resources. It may be necessary for the client's legal counsel to provide wording that is suitable.

- **Identify Incident Handling team and primary contact**
  The client should have a named response team. A team leader should be assigned as the primary contact point for Quest Managed Services to contact in event of an incident. After hand-off the team is then responsible for the expeditious response to identified security incidents.

- **Identify Client Management Contacts**
  Quest should understand the organization structure and appropriate management contacts. Additionally, Quest Managed Services should possess an escalation procedure, which identifies who should be called and when, as security incidents are identified.

- **Develop standard and emergency communications plan**
  Under ordinary circumstances communication between security response team members and management may be accomplished via the standard

communications methods (e.g. inter-office telephone, email, etc.). However, more extreme circumstances such as a breach that has compromised the IP-based telephone system or email service will require alternate methods of communication. A current listing of cell phone or alternate contact numbers are required from each client. Due to the inherent risks introduced by cell-phone communication, no Quest employee will request passwords from a client via cell phone communication.

- **Provide reporting facilities**
  What data is collected and for how long will be addressed during the preparation for managing a client's infrastructure. Reports will be provided to each client based on the agreed parameters of the Managed Services agreement.

- **Develop interfaces to law enforcement agencies and all Client Incident Response Teams**
  Serious incidents may require the involvement of law enforcement agencies. This will become more of a requirement as laws are passed which require the reporting of certain types of intrusions or breaches. Clients are responsible for notifying the appropriate authorities as they deem necessary.

Prevention

- **Harden systems, networks applications, and facilities**
  Managing security for the networked resources is an ongoing process of updating and upgrading systems, networks, and applications to defend against intentional and unintentional threats to these resources. These changes are identified in several ways, for example:

  - Vendors regularly release fixes for security vulnerabilities. These fixes are to be applied by the security management team
  - Security management institutions also publish identified vulnerabilities from which other security management professionals benefit

  Further system fortification is usually part of an incident resolution to avoid similar situations in the future. Having determined how an incident occurred, the team is then responsible for assuring the incident is not encountered again.

Managed Services staff is responsible for updating resident Quest applications and systems, as updates are available. Unless otherwise stated in the Managed Services agreement, Quest is not responsible for notifying clients when new threats are identified or security updates are available. As a courtesy, Quest will occasionally notify clients of potential threats and security updates available, but Quest is in no way responsible for performing such notifications on a regular basis.

- **Modify policy, processes, and/or procedures**
  In some cases the vulnerability may be policy, process, and/or procedure related. Some examples may be; insufficient password policy, inappropriate sharing of userids and/or passwords, system consoles left unattended, administrator accounts using default passwords, etc.

  Clients are solely responsible for and policy, process, or procedure modifications for their infrastructure. Where applicable, Quest should be made aware of changes that will affect how the environment is managed.

- **Upgrade security applications**
  Security tools are only effective when they are kept current. This is an ongoing effort that requires Quest be vigilant in acquiring and implementing patches and upgrades that enhance security.

Identification

Incident Identification may be accomplished in a number of ways, such as:

- Alert(s) received from Management Application(s)
- Managed Services log scans
- User(s) encounter and report system anomalies
- Vendor Security Advisory

It should be noted that Identification involves not only in determining whether or not an incident has occurred, but also in keeping up-to-date on emerging security threats.

- **Assign personnel to monitor security applications**
  A Quest Managed Services employee will be assigned as the primary monitor of the security management tools during business hours. The support personnel are responsible for the following:

  - Daily health checks of the managed security devices and applications
  - Monitor security console for incoming security alerts
  - Review received alerts

- **Classify the incident**

  The Managed Services staff will classify the incident based on known facts. Classification of the event is necessary to determine next steps and the swiftness of the staff's response. This information will also help formulate the severity level, which will help the client's security team prioritize their efforts.

  - Vulnerability – System, network, or application security deficiency determined by support staff or via vendor notification.
  - System Intrusion – Unauthorized access to an information system from and internal or external source.
  - Malicious Code – Virus, Worm, or Trojan Horse
  - Denial of Service – Actions which prevent any part of an information system from functioning in accordance with its intended purpose, to include any action which causes the unauthorized destruction, modification, or delay of service.
  - Probe – Consists of any attempt to gather information about an information system or its users online.
  - Physical – Personnel, facilities, materials, equipment, and information.
  - False Alarm – Initially, incidents will be classified in one of the above categories. After investigation, the incident response team may be reclassified to this category.
  - Hoax – As with False Alarms, after a thorough investigation, the incident response team may reclassify an incident under this category.

- **Assign a severity to the incident, based on known facts**

  The Quest Managed Services staff will assign a severity level to the incident in the security incident report. The severity level may be adjusted up or down as additional information is discovered and the event ramifications are known more thoroughly.

  - **Level 1** – Custom level designated for further event correlation.
  - **Level 2** – Low threat level, such as, unsubstantiated rumors or security threats.
  - **Level 3** – Threat of future attacks, vendor (or another reliable source) that describes discovered vulnerabilities, or detection of reconnaissance.
  - **Level 4** – This includes incursion on non-critical system(s), detection of a precursor to a focused attack, or substantiated threats of imminent attack.
  - **Level 5** – Incident has impacted critical systems, networks, and/or applications. Or, the incident could have long-term implications for executing normal business processes.

- **Maintain a provable chain of custody**

  Quest will maintain records of the received alerts for the time period specified in the Managed Services agreement. Ad-hoc reports may be generated at the client's request to support any documentation efforts they may have for an incident.

- **Contact client's security representative**

  Based on the parameters set forth in the Managed Services agreement with the client, Quest will notify the client when alerts are received. The level of alert, which will require a notification to a client, will vary.

- **Notify client management if appropriate**

  Whenever an alert of the severity specified in the client communication plan occurs, a Quest staff member will notify client management of the incident.

Follow-up

After an incident has been fully resolved and all systems are restored to a normal mode of operation, a follow-up (postmortem) analysis should be performed. If opportunities are available for enhancing the security of the environment, the client may work with Quest to take the appropriate actions. If required, Quest will provide the client and/or law enforcement with the appropriate alert streams or log data necessary.

Quest-Pondera team goals for customer support include the following:

Provide high-quality operations support. Quest has local first-line infrastructure support personnel available to investigate and resolve application, server, network, and security infrastructure issues as they occur. In many cases, the NOC will be able to immediately restore service through a redundant or alternate component, and the local support team will resolve the issue promptly. We maintain relationships with the infrastructure hardware, software, and network services vendors to allow for urgent callout service to resolve more complex issues.

Take a business impact perspective. We will focus on a business-oriented design approach that will make it easier for stakeholders to understand and be involved in the process. Rather than following boilerplate procedures, we approach maintenance, operations, and infrastructure support as a partnership.

Leverage ITIL leading practices. We will leverage ITIL standards for design change management, configuration management, asset management, service desk, and business continuity processes. We will focus on reusing existing toolsets as much as possible, which will help manage costs and maintain a smooth operating environment.

8.7 Migration and Redeployment Plan

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.***

Pondera will maintain the FDaaS services until no longer contractually obligated. All of the Purchasing Entities' data will be destroyed in accordance with NIST 800-88 Guidelines for Media Sanitization within 30 days of contract end. All security measures will be maintained by Pondera to secure the data until the data is completely destroyed, even after no longer contractually obligated to maintain the service/contract end.

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.***

When Pondera is no longer contractually obligated to provide service, there will be no data returned to the Purchasing Entity data (per 8.7.1 above) along with any 3rd Party cross-match data and all analytics will be purged.

8.8 Service or Data Recovery

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).*

The Quest-Pondera team's response to (a) extended downtime, (b) unrecoverable loss of data or (c) a system failure are dependent on the level of engagement outlined in the client's SLA. It depends on the customer's policies for data backup and restoration. Services outside of the SLA are billed as Time and Materials. (d) The customer would need to select a restore time of 4 hours as a part of Quest's Disaster Recovery as a Service (DRaaS). Quest-Pondera can accommodate a recover a restore time of 4 business hours if that is what is defined in the customer SLA at the appropriate support level and rate for that service offering.

The RPO and RTO are provided by the customer and the appropriate service levels are delineated in the SLA. Quest can consult with the purchasing entity to create a service plan to meet client expectations.

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

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

Quest-Pondera provides a sophisticated network data backup, storage and recovery system in order to backup Quest's critical systems as well as providing the client's backup, storage and recovery needs.

Methods of data backups and server image backups:

Utilizing the latest storage technology of disk to disk and virtualization from two of the leading storage and recovery companies in the industry, Quest backup procedures encompass several varieties of full and incremental backups to secure Quest's and client's data on a continual basis.

Digital location of backup storage:

This technology allows Quest the opportunity to maintain a higher level of service in terms of multiple data depositories, off site vault storage, increase speed of data retrieval and the flexibility to be interchangeable depending on the client's needs. In conjunction, and where specified in the client's SLA, Quest provides additional off-site backup facilities to provide a secondary copy of the appropriate backups, further diminishing the risk of data loss.

8.9 Data Protection

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.***

All data transmitted to Pondera's secure Data Center at Quest is transferred using Secure File Transport Protocol over a Site to Site VPN. All data received by the Purchasing Entities from the Quest Pondera team is transferred using Secure File Transport Protocol and/or https (SSL) over a Site to Site VPN. FDaaS itself is only accessible via the Site to Site VPN and is not accessible in any way over the internet.

All data at rest is stored on a solid state fully-encrypted SAN.

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.

Quest-Pondera can review and discuss relevant and applicable Business Associate Agreements or other agreements required by a Purchasing Entity.

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.

Pondera's sole use of the source/government data is to provide the services defined in the Master Agreement, participating addendums, and related services described in the SLA (Service Level Agreement) and DUA (Data Use Agreement). Any and all source/government data obtained will not be resold or distributed in any way.

8.10 Service Level Agreements

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*.**

Quest-Pondera's Service Level Agreement is customized to reflect the services and components requested by each client. Quest-Pondera and the Purchasing Entity will work together to document service requirements. The SLA contains Terms and Conditions that can be reviewed and discussed as it relates to specific Purchasing Entity requirements.

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.***

A sample of the Service Level Agreement is provided as part of this response.

8.11 Data Disposal

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

Physical destruction will be the primary method to dispose of digital media and data storage devices contained in equipment that will be transferred externally.

Digital media may be incinerated, shredded, crushed, or pulverized and sent for recycling. Quest will remove digital storage devices from computing and mobile device equipment before it leaves the Quest warehouse for disposal. Quest will lock digital storage devices in a secure area until they are retrieved by a contracted vendor for destruction.

8.12 Performance Measures and Reporting

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

The following table shows the Quest-Pondera Server/Platform Uptimes (excluding planned maintenance windows):

Server Type	Server Uptime %
UNIX/LINUX	99.99999%
Windows	99.9999%
Mainframe	99.99999%

If purchasing entity has some specific critical application needs, Quest-Pondera will work with purchasing entity to identify and establish the appropriate Service Levels.

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

Per the Quest Service Level Agreement Appendix A – Data Center Facility Standards and Warranty, the following criteria apply for standard uptime service:

Force Majeure Event: any act of God, fire, casualty, flood, war, terrorism, strike, lock out, failure of public utilities, injunction or any act, exercise, assertion or requirement of any governmental authority, epidemic, public health emergency, destruction of production facilities, insurrection, inability to obtain labor, materials, equipment, transportation or energy sufficient to meet needs, or any other cause beyond the reasonable control of a party.

Service Interruption: a complete loss of signal that renders the services unusable.

Planned Service Interruption: any service interruption caused by planned work such as scheduled maintenance or planned enhancements or upgrades.

During the term of this SLA, Quest warrants that (i) the services will be available 99.9% of the time per calendar month and (ii) if the services are not available, with the exception of services impacted by Internet performance or availability, Quest's liability for any service interruption (individually or collectively, "liability"), shall be limited to the amounts set forth in Table 1 below. For the purposes of calculating credit for any such liability, the liability period begins when Client reports an interruption in any portion of the service to Quest, provided that the liability shall be deemed resolved upon the closing of the same trouble ticket or the termination

of the interruption, if sooner, less any time Quest is awaiting additional information or premises testing from Client. In no event shall the total amount of credit issued to Client's account on a per-month basis exceed 50% of the total monthly charges. Service interruptions will not be aggregated for purposes of determining credit allowances. To qualify, Client must request the credit from Quest within 30 days of the interruption. Client will not be entitled to any additional credits for service interruptions. Quest shall not be liable for any liability caused by force majeure events, planned service interruption, or as a result of Client's acts, omissions, or equipment. Service credits will not entitle Client to any refund or other payment from Quest. Service credits may not be transferred or applied to any other account.

THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE CONCERNING MERCHANTABILITY, TITLE, OR FITNESS FOR A PARTICULAR PURPOSE, AND NO REPRESENTATION OR STATEMENT NOT EXPRESSLY CONTAINED IN THIS SLA WILL BE BINDING ON THE CONSULTANT AS A WARRANTY. THIS APPENDIX A STATES THE ENTIRE LIABILITY OF QUEST AND THE EXCLUSIVE REMEDY OF CLIENT WITH RESPECT TO QUEST'S BREACH OF ANY WARRANTY HEREUNDER.

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.***

If engaged by the customer to do so, Quest can offer Help Desk as a Service as part of the client's SLA. Quest Managed Services clients have 7x24x365 to Quest's Network Operations Center (NOC). Clients may send a support request in a secure manner to performance@questsys.com or by telephone to 800-443-5605. Quest NOC engineers will categorize the ticket according to urgency level. Quest engineers have ITIL and ITSM training.

Ticket Urgency Levels. Support, alert, or Client requests will be assigned a ticket and issued an urgency level based on priorities which are determined by request type and level of impact.

Low. Informational request; no issues are present or no services are impacted. For example, "What is your data center address?"

Med-Low. An issue or event may be impacting a single user who is able to work, or a workaround was provided. For example, “I'm unable to access questsys.com using internet explorer, but I can access it using Firefox.”

Medium. A monitored device is deemed non-responsive by the monitoring tool. For example, “A monitored device is reporting a “packet loss” or is inaccessible and non-responsive to triage/troubleshooting commands.”

Medium-High. An issue impacting the entire site, department, or multiple users for which no work around is available. For example, “The Sacramento office is unable to connect to the internet.”

High. An issue impacting the entire company or multiple sites for which no work around is available. For example, “No one in our company is able to get to email or make a phone call.”

Quest’s Service Level Agreement Incidents, Response Time

- **Incidents and Emergencies**. If any incidents or emergencies occur, Quest will utilize the incident management process as defined in the 60-day profile. Quest will respond to and resolve all incidents within the timeframes and according to the methods set forth in the 60-day profile. To report an incident or emergency, Client shall send an incident notification in a secure manner to performance@questsys.com or by telephone to 800-443-5605.

- **Problem Response Time:**

  The problem response time is the time period starting after (i) Quest’s confirmation of the service event and (ii) receipt of the information required from the Client for Quest’s support team to begin resolution and open a trouble ticket in Quest’s systems. Due to the wide diversity of problems that can occur and the methods required to resolve them, problem response time IS NOT defined as the time between the receipt of a call and resolution of the problem. After receiving a report of fault, Quest shall use a reasonable method to provide the Client with a progress update(s).

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

The following table represents SLA remedies for Data Center Facility Standards and Warranty.

SLA Appendix A Table 1

Length of Service Interruption	Amount of Credit
< 40 minutes	None
40 minutes – 4 hours	5% of total Monthly Charges
4 hours – 8 hours	10% of total Monthly Charges
8 hours – 12 hours	20% of total Monthly Charges
12 hours – 16 hours	30% of total Monthly Charges
16 hours – 24 hours	40% of total Monthly Charges
24 hours or greater	50% of total Monthly Charges
THE TOTAL CREDIT ALLOWANCES PER MONTH ARE CAPPED AT 50% OF THAT MONTH'S MONTHLY CHARGES FOR THE INTERRUPTED SERVICE. SERVICE INTERRUPTIONS ARE NOT AGGREGATED FOR THE PURPOSES OF DETERMINING CREDIT ALLOWANCES.	

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

Quest-Pondera utilizes the following process for maintenance as per the Quest Service Level Agreement.

Maintenance. A maintenance window is a defined period of time during which planned outages and changes to production services and systems may occur. The purpose of defining standard maintenance windows is to allow Client to prepare for possible disruption or changes. The following process will be utilized for the updating of services.

- **Updates/Patches.** Updates will be implemented during the scheduled maintenance windows defined in the "60-day profile" described in Appendix B attached hereto. Prior to implementing any updates, Quest will send an email to Client notifying Client of the update, when it will be implemented, and its impact.

- **Changes.** If configuration changes to the components are required or requested, Quest will utilize the change management process as defined in the 60-day profile. Any changes requested by Client will be completed

within the request resolution timeframe set in the 60-day profile and implemented during the scheduled maintenance window as defined in the 60-day profile. To request a change, Client shall send a change request in a secure manner to performance@questsys.com.

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

For Disaster Recovery services, Quest-Pondera offers DR as a Service as an additional service that can be added to the client's SLA. The SLA remedies and metrics would be delineated as part of the service engagement. As a software only solution, Quest's DRaaS does not require any changes to current environments or downtime to implement. With Quest Managed Services your business platforms, applications, and functions are monitored and managed. In the event of a declared disaster, Quest services are available around the clock.

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.***

Quest-Pondera Managed Services clients receive the reports defined in the Service Level Agreement. Standard reports are batch statistics generated and published on a monthly basis. Quest-Pondera also offers Managed Services Clients access to a portal for real-time statistics and monitoring tools.

Please refer to the file Dashboard-Monthly Sample.

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

Quest-Pondera Managed Services clients will receive monthly reports as mutually defined in the Service Level Agreement. Electronic copies of reports are delivered by email from Quest to Managed Services clients. Custom or ad-hoc reporting can be further defined in the SLA or provided on a Time and Materials basis.

Quest has established information system processing procedures for the control environment in which Quest's monitoring efforts are conducted. Our approach enables rapid response to a performance event when it occurs, and allows for proactive measures to be taken if thresholds that can affect performance, such as capacity utilization, are about to be reached.

Monitoring Performed:

Utilizing industry standard tools, the Quest NOC monitors network devices, servers, VoIP, applications and custom devices for a wide range of metrics. These include uptime, packet loss, saturation, bandwidth, storage, services, protocols, disk space and many more.

Measuring System Performance, Usage, Availability:

Quest generates standard reports and well as customized reports to illustrate adherence to contracted SLAs and KPI metrics. Attached is a sample file named "Dashboard – Monthly.xls".

Possible Methods of Delivery:

Delivery methods are adjustable to client's needs. Reports are presented by email, dashboards, as well as selective real-time reporting.

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

Quest-Pondera Managed Services clients have access to Quest's Network Operations Center 7x24x365.

Escalation Process:

Quest has documented its customer support procedures to outline the process of working directly with customers on requests, work orders and trouble tickets. The procedures include, but are not limited to, the following:

- Incoming calls answered 24x7 by NOC technical staff.
- Each call is logged by the technical staff and the client's automated case file is reviewed for an existing case related to the current problem.
- The case file is updated to reflect the pertinent details of the call and the resolution process started.

If case cannot be resolved, the case is assigned to the Specialist Support Group for resolution.

Quest receives customer support information via email and telephone. Quest uses a trouble-ticketing application to manage all client and internal trouble tickets and change management issues. The application provides:

- Support ticket management
- Standard problems and resolutions
- Speed Search
- Reporting
- Knowledge management
- Escalation management
- Web self-service option

Peak Period Response:

Quest can work with the client to determine peak periods and proactively work with the client to ensure that additional staffing or services are in place to address increased workloads. The details of peak-period response requirements shall be documented in the SLA.

Client Call Processing:

Quest uses a defined workflow for responding to client calls to the Managed Services Operation Center. The guardianship process describes how incidents are tracked by Quest Managed Services through the entire incident lifecycle. A sample flow-chart titled Quest Managed Services Client Call Process.pdf is submitted with this response.

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

Quest-Pondera Managed Services clients may scale-up or down as necessary. The change request procedure is defined in the Service Level Agreement. If configuration changes to the components are required or requested, Quest will utilize the change management process as defined in the 60-day profile. Any changes requested by Client will be completed within the request resolution timeframe set in the 60-day profile and implemented during the scheduled maintenance window as defined in the 60-day profile. To request a change, Client shall send a change request in a secure manner to performance@questsys.com. The change request is managed by Quest's NOC engineers who are available 7x24x365.

The request for additional and/or new services ("new/additional services") can be made via email and/or phone call to the Quest primary points of contact. Any new/additional services added to this SLA will be documented via a separate addendum to this SLA. Services provided within subsequent addendum(s) will

adhere to the terms and conditions of this SLA, unless otherwise specified within the addendum. Quest will obtain written Client approval and/or a purchase order for any new/additional services. Upon Client approval, all references to services shall include all approved new/additional services. Quest is authorized to make adjustments to the fees and surcharges charged for the services in order to cover the costs of any new/additional services. Cost and fee adjustments will be documented via email and/or a separate addendum and sent to Client prior to fee adjustment. Client agrees to pay the fees and surcharges for the services, as adjusted.

8.13 Cloud Security Alliance Questionnaire

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 of CSA STAR Continuous Monitoring*.

Quest has submitted the Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B as part of this response. File: Exhibit 1 to Attachment B CAIQ Level 1 CSA STAR Registry.

8.14 Service Provisioning

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

In the event that a client requests an implementation in fewer than 90 days from receipt of data, we do our best to accommodate their requirements. In the past we have implemented a limited set of flags in a shortened timeframe, choosing a small number of flags that provide the greatest impact to the program and investigative team. Because we are offering a Software as a Service solution, we can add new flags to a deployment at any time. In this situation, we would recommend beginning with the top 5 flags and adding the remaining flags over the next 3 months. This helps maintain the quality of the implementation.

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

The standard lead time for provisioning our Cloud Solutions Software as a Service is 90 days from the receipt of data. We anticipate that the Security plan and data preparation will take approximately 30 days, and 90 days later we anticipate

"turning on" the solution. This provides adequate time for data to be reviewed, flags and alerts to be tested, and investigative teams to schedule training.

8.15 Back up and Disaster Plan

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

The retention policies between Quest-Pondera and the purchasing entity will be documented in the Service Level Agreement to conform to required legal retention periods.

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

Quest's Roseville High Availability Business Center (one of over two dozen Global Service Delivery Centers) is strategically located at one of the most seismically stable and secure locations in California. It is uniquely situated in an area located well above the flood plain, clear of any mudslides or forest fires and far enough inland from extreme weather. Quest's Managed Services use a follow-the-sun model where client services are provided from multiple sites within the United States including California and Florida. Should the primary data center become unavailable, Network Operations failover to West Palm Beach FL or to Quest's Service Delivery Centers.

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.*

Quest has a network of over two dozen Service Delivery Centers across the nation to support redundancy, failover and the ability to run large scale applications independently in case one data center is lost.

Continuity Planning and Recovery

Quest places a high value on providing continuity of service to its clients. The plans are designed to address issues that could arise assuming a worst-case scenario were to take place. Use of this strategy alleviates the need to plan for a myriad of situations, and degrees of severity, which can never be fully defined is considered a best practice planning approach. This philosophy yields a capability whereby each situation can be readily assessed and actions tailored as required to address

the issues at hand. Quest's disaster recovery plans stand ready to be activated should an event affect the Service Delivery Center and cause a disruption.

Quest's disaster recovery philosophies emphasize disaster prevention, mitigation, and recovery. The work environments are regularly reviewed to identify potential sources of risk. Management continually strives to reduce potential single points of failure as part of this process through an analysis of the operations monitoring procedures. Technology personnel also evaluate changes made to the environment or whenever new services are introduced. Continuity plans and solutions are implemented wherever necessary, and improved on when possible, to reduce the likelihood of significant interruptions in service capabilities.

Disaster Recovery Plan

Quest Managed Services has developed a Disaster Recovery Test Plan for its Service Delivery Center. The plan addresses the following: Goals and Objectives, Roles and Responsibilities, Disaster Recovery Test Scope, Resource Coordination, Recovery Site Setup, Hardware Configuration, Application Recovery, and Application Functionality Testing. The test plan is designed to ensure the appropriateness of the disaster recovery and business continuity processes and procedures through validation and verification (testing) and to ensure that the program/project team is aware of these processes and is prepared to implement them when needed. Frequent and comprehensive testing is performed to ensure that Quest is fully prepared to respond to an actual disaster event. Furthermore, the testing is used to validate the accuracy and efficiencies of the support documentation.

In the event that the NOC is lost, the corporate office may be used to temporarily provide security and network monitoring services.

Quest's Disaster Recovery Plan is included within Quest's "Business Continuity Plan" (BCP). The procedures included within the Disaster Recovery Plan included: Disaster Declaration, Managed Services Disaster Recovery Teams, Backup Strategy, Recovery Plans, Non-Catastrophic Recovery Plans, Task Cross-Reference, Operations Procedures and Training. Recovery of the client configuration is performed to enable security monitoring as quickly as possible. Once all systems are recovered, the recovery team moves to the validation phase to ensure the integrity of the system. As a final point, recovery support is performed until all systems are fully stabilized.

Quest DR Plan addresses their operational systems only. It does not cover client systems. The recovery of the clients systems are addressed per their individual SLA.

8.16 Solution Administration

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

FDaaS can be configured by way of a custom "UserManager" role to allow the Purchasing Entity to lock, unlock, and issue password resets to the FDaaS system, however, Pondera maintains all FDaaS account creation and assignment of roles as part of the Software as a Service (SaaS) solution.

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

Quest-Pondera provides several options for Virus Protection for data stores through strategic partnerships with leading anti-virus vendors, giving customers a choice of enterprise-class anti-virus solutions to be installed and configured. These world-class anti-virus engines are the same used in their respective commercial products, ensuring that your company is strongly protected against dangerous viruses and other types of malicious code. Yes Quest-Pondera does offer anti-virus protection as a service. A Purchasing entity can elect to add anti-virus as an additional service to the SLA for an additional monthly recurring charge.

Continuous virus-detection updates

Quest's Virus Protection is updated as our anti-virus vendor partners create new virus definitions. A Dynamic Update Service guarantees that Virus Protection is always up-to-date, providing the maximum defense against viruses—and minimizing the burden on IT administrators. Quest's anti-virus partners provide some of the fastest product-ready anti-virus updates in the industry, and the Dynamic Update Service makes them available to you immediately.

Integrated, centralized administration

Quest's anti-virus module is fully integrated into our message processing platform, providing complete control over virus protection through a unified interface. Quest lets you configure all aspects of virus protection—including virus filtering activity, detection and cleaning processes, disposition options, and reporting—with the same interface used for spam and content compliance administration. Administration duties can also be optionally delegated to other groups. For

example, while IT may manage general email and anti-spam settings, a corporate security group could selectively manage anti-virus settings.

Enterprise-grade Virus Protection

Quest's anti-virus functionality protects your enterprise from harmful viruses. Our Virus Protection provides the utmost protection and efficiency by employing the following three-step process:

- Policy definition Our Virus Protection lets you create new anti-virus policies or easily import existing virus protection policies.
- Real-time monitoring Quest's Virus Protection efficiently monitors the email stream for virus threats while definitions are automatically kept up to date through our Dynamic Update Service.
- Custom dispositions Our Virus Protection gives your enterprise the flexibility it needs to classify and route messages based on numerous virus detection message states, such as sending infected messages to quarantine or stripping destructive attachments.

Service Benefits

- Industry-leading anti-virus vendors: the choice of leading anti-virus solutions provides the best enterprise defense against email-borne viruses.
- High-performance processing Virus detection is completely integrated into the overall message analysis allowing the message to be opened only once while it is checked for spam, virus, or content-compliance issues. The addition of virus protection does not impact the scalability of Quest's solution.
- Continuous protection: our Virus Protection continuously polls a Dynamic Update Service for anti-virus engine updates. The polling interval is completely configurable to ensure that your enterprise stays protected from the latest virus threats.

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

In the past, Pondera has successfully migrated our entire cloud infrastructure from a previous Cloud Hosting solution provider to Quest without any customer interruption. There are no future plans to move to a different Cloud Hosting Provider than Quest, but Pondera is fully prepared to do so if an unforeseen need arises.

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

The "UserManager" role can be assigned to as many different participating entities as desired. Each User Manager can have their account configured to manage only specific groups of users.

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

Pondera can apply administration policies to FDaaS including but not limited to minimum password length, password complexity, password expiration policy, user access hours, Site to Site VPN settings, and session timeout length.

8.17 Hosting and Provisioning

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

There are many factors that will influence the client's migration to "XaaS", the strategic planning should be a living roadmap that requires regular evaluation and realignment to account for the organization's goals. Quest-Pondera will work jointly with the client to categorize their information systems, users and applications as low-impact, moderate-impact, or high-impact to meet the security objectives, confidentiality, integrity and availability when adopting XaaS as a new business capability. Using the FIPS framework as reference, services will be mapped to the most cost effective solution(s) while limiting company security exposure and impact.

<u>Migration from On-Prem to Cloud Services:</u>

Systems tagged as low and moderate are ideal candidates for quick transition to a XaaS platform. Initially focusing on Infrastructure applications services such as Active Directory, Email services, introduction of a user virtual desktop, secure Wide Area Network (WAN), hosted SOC, etc.

Quest would position a highly secure and encrypted WAN using Quest Cloud services. Each site would have two redundant circuits separating data across one circuit and communications such as voice, video, instant messaging across the other. If applicable, a 3rd telecommunications infrastructure is available with diverse paths. Email services, video, instant messaging and voice services will be consolidated to a Microsoft platform and provided back to the company through a

consumption-based model enabling cost transparency and elastic growth flexibility.

Site-to-Site communications across both WAN circuits will be encrypted and controlled by the client to assure compliance requirements. Non-engineering users will be identified in preparation of migration to a full redundant and secure Virtual Desktop Infrastructure (VDI).

If application capability permits, application access will be load-balanced using geo load balancing between East and West assuring user performance is as optimal as possible. The introduction of a cloud-based application hosting model will mitigate three assumed business risks. It will remove any “hub and spoke” architecture remedying any single point of failures, provide a Disaster Recovery solution and centralize application change and audit to key central locations.

Internet access will be tightly regulated and consolidated to the Quest Cloud, removing existing the client internet circuits. All inbound and outbound internet traffic will be monitored through Quest’s Federal SOC and in concert with Quest’s Network Operations Center (NOC), Quest will introduce a Data Loss Prevention (DLP) and Network Access control (NAC) service through Quest’s Federal SOC.

By adopting a XaaS centralized hosting model, company costs will greatly reduce, streamlining compliance frameworks such as NIST, DFARS, AR25-2, etc. by reducing risk and managing changes to a central location. Overall regulatory and compliance can be as strict or as flexible as the company requires. Quest is capable of providing highly secured, scalable, tightly integrated services. Security will be enforced from top-down from the SOC and in alignment with the Network Operations Center (NOC) the company overall Infrastructure services, Risk, and Control will be monitored and controlled from one location.

<u>Transition Process: Implementation/Migration Plan Development.</u>

As part of the transition process, Quest will closely work with the client to develop an Implementation/Migration plan that will include a provision for post-migration health checks to evaluate both design and project goals. Implementation/migration plan development will include analyzing any changes for which the client operations staff should be alerted.

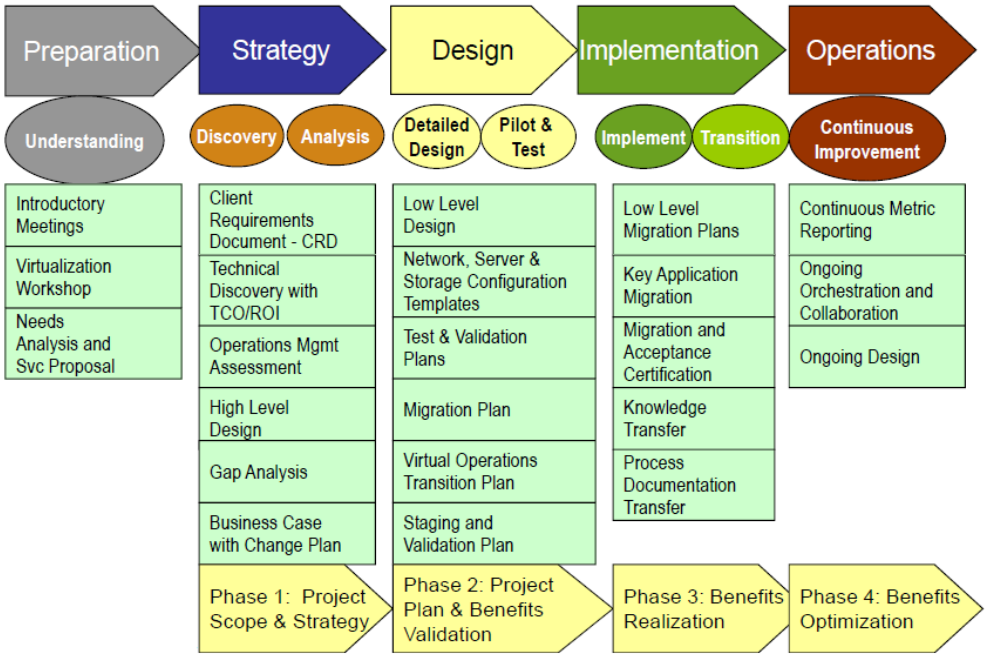
Quest will create and provide the implementation and migration plan. The Implementation and Migration Plan Document will include: a). step-by-step procedures required for a successful implementation and migration; b). scripts for

required implementation and migration procedures; c). fall back plans, in the event a portion of the implementation and migration is not immediately successful; d). validation to ensure that an implementation and migration is successful; and e). recommendations for the implementation and migration sequence and scheduling timeline for the implementation.

If applicable, Quest will document any client-provided plans for implementation and/or migration, identifying any gaps.

Quest then reviews the Implementation and Migration Plan Document with the client for comment and approval before it is formally completed and released.

The process is listed in more detail below:



8.17.2 *Provide tool sets at a 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 0 and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources)*

Quest-Pondera can work with client to provide tool sets for various actions including (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 and (3) Securing additional storage space. These are not automatically included, but Quest-Pondera can review requirements and provide as part of contractual services.

Quest-Pondera offers Managed Services Clients access to a portal for real-time statistics and monitoring tools for use by each jurisdiction's authorized personnel covering components of a public (respondent hosted) and hybrid cloud (including Participating entity resources).

8.18 Trial and Testing Periods (Pre- and Post- Purchase)

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

Pondera Solutions, Inc. employs a hosted User Acceptance Test, or UAT environment that is initially populated with historical production data from the client. After the initial historical data release, releases on a monthly basis or at least multiple times per year refresh the UAT environment. Pondera employs automation tools to handle any of the following QA (quality assurance) tasks: unit testing, functional testing of key application interfaces, testing of SOA interfaces and performance testing of the application running on the cloud services platform. While testing automation delivers optimal results in terms of the speed at which testing can be executed, Pondera also performs testing by subject matter, including but not limited to, unit testing, regression testing, sanity testing, acceptance testing, and usability testing.

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.*

Pondera Solutions, Inc. employs a hosted Fictitious FDaaS environment to allow clients of similar governmental services (i.e. SNAP, Unemployment, Tax, etc.) to preview the capabilities and functionality available in FDaaS within a particular service area and/or over multiple service areas. As new or requested functionality is available, clients will have the opportunity to test and/or be trained using the new or requested functionality in the hosted Fictitious environment. This allows for clients to confirm mandatory requirements can be met.

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

Pondera offers unlimited support and training for our clients. Training includes instructor led group training and one on one training sessions in person, via the web, or by any other means necessary.

Pondera's FDaaS training is a two-day course conducted on site. During this course, we provide an overview of the fully customized FDaaS system using actual production data, wherever possible. In other words, we conduct the training on the actual system you will be using. We begin with an overview of the system functionality, basic navigation, and a demonstration of how to customize the portal for each user's individual needs. We then run through use-cases to demonstrate how to incorporate the system into your processes and daily activities.

Class participants are provided with the slide presentation and screen-specific user manuals.

After attending this training, users are expected to understand how to navigate, customize, and use the FDaaS system. This includes handling Alerts, using Geospatial Maps, conducting Network Analysis, reviewing Provider and Beneficiary Profiles, and understanding the Super Search function.

Pondera's FDaaS support includes multiple channels for FDaaS users including Telephone, Electronic, and On-site Support. These channels support user system inquiries, system bug logging and tracking, and system enhancement requests.

Regardless of the channel, all issues are logged into a single database. This provides the Client and Pondera with a single comprehensive view of all system bugs and enhancement requests. Pondera will track the time to resolution for all issues logged by the State Agency and report them to the State Agency during our regularly scheduled Quarterly Meetings or on an ad hoc basis, as required by the State Agency.

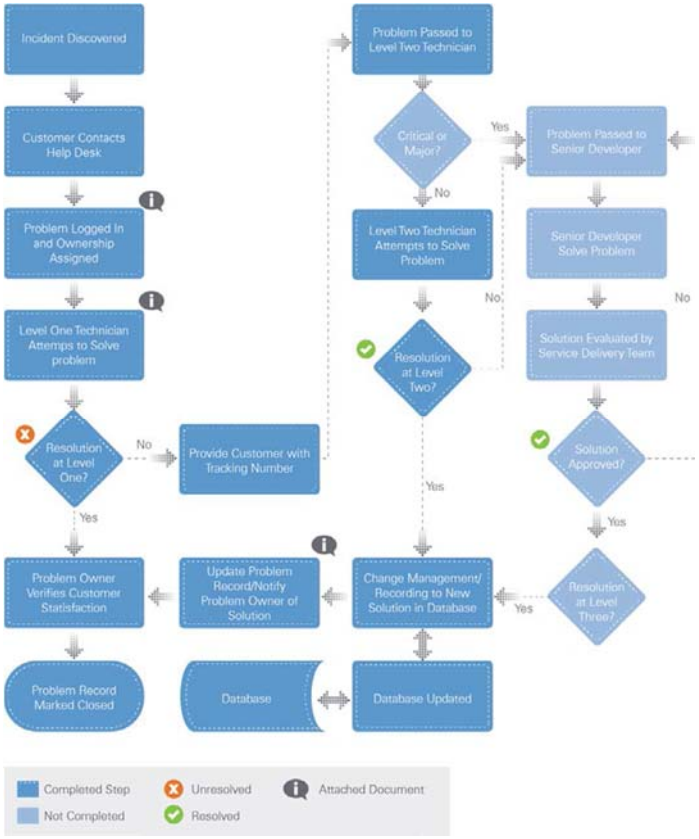
Pondera's Special Investigations Unit (SIU) provides first-level support services. The reason for this is twofold:

1. The SIU uses the FDaaS system every day to conduct their jobs including to research investigative reports. Their familiarity with the system is extremely helpful to FDaaS users with questions.

2. The majority of questions that come to the help desk are functional issues and enhancement requests. The SIU is ideal to field these calls. For technical questions, they simply capture the required information and enter a log in the issue tracking and resolution system.

Calls to the help desk will be answered by a member of the SIU and will be conducted in English. The SIU member, like all Pondera employees, will follow our HIPAA and other security training and testing processes.

Our process is a closed-loop process. It routes issues through a series of escalation steps with the goal of handling as many issues as possible on the first call. Regardless, when the issue is resolved, a member of the SIU contacts the State Agency to ensure that you are satisfied with the fix.



8.19 Integration and Customization

8.19.1 *Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.*

The Quest Pondera Fraud Detection as a Service (FDaaS) solution is comprised of many tightly coupled modules that are integrated using a combination of REST and SOAP services. These services can be exposed to other 3rd party applications as desired. For example, if a participating entity has an existing case management system, FDaaS can be integrated seamlessly with existing REST and /or SOAP services. In addition, our Fraud Detection as a Service (FDaaS) solution is designed to interoperate with a variety of Off the Shelf or custom built applications. The FDaaS data export feature will allow users to export data in Excel, .cvs, Predictive Model Markup Language (PMML) or any other format. We can also import data from a variety of sources or applications.

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

The Pondera Fraud Detection as a Service (FDaaS) solution is a highly customizable off the shelf product. While FDaaS is an existing product, it is also highly configurable to meet each Participating Entity's unique requirements. These can include, but are not limited to, flags for behaviors that are unique to the program or the state, implementation of rules and benchmarks that are unique to the program or state, and scorecards that reflect the programs unique characteristics.

8.20 Marketing Plan

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

We intend to market our Solution to NASPO ValuePoint and Participating entities in a number of different ways. We anticipate a social media campaign, press releases, and outbound direct marketing. We also hope to include NASPO ValuePoint information on our website and marketing collateral. In addition, we would like to go out for field visits to participating states. This would include sales calls, Software demos, and additional marketing activities.

A complete marketing plan has been attached at the end of this proposal as NASPO Marketing Plan.pdf.

8.21 Related Value-added Services to Cloud Solutions

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

Quest/Pondera offers a Software as a Service solution with little need for additional value-added services. We would like to offer supplementary investigative support and internal process improvement consulting to our NASPO ValuePoint clients. These items are more fully described in our Pricing document.

8.22 Supporting Infrastructure

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

We do not anticipate any additional infrastructure to be required. Our solution is a hosted software as a service model and thus would not require any additional supporting infrastructure by the Purchasing Entity.

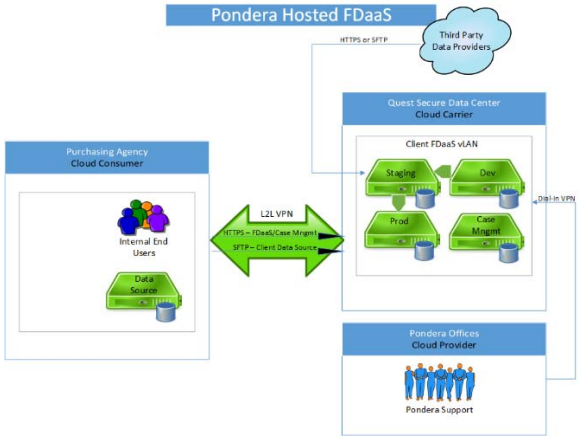
8.22.2 *If required, who will be responsible for installation of new infrastructure and who will incur those costs.*

We do not anticipate any new infrastructure to be required and thus we do not anticipate any incurred costs.

8.23 Alignment of Cloud Computing Reference Architecture

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

FDaaS is a Software as a Service (SaaS) installed in a Platform as a Service (PaaS) environment. The cloud consumer is the purchasing agency, the cloud provider is Pondera Solutions, and the cloud carrier is Quest Technology Management. See diagram below:



Confidential, Protected, or Proprietary Information

None.

Exceptions and/or Additions to the Standard Terms and Conditions

None.

Quest
TECHNOLOGY MANAGEMENT

Christopher Hughes, Assistant Director
State of Utah, Division of Purchasing
christopherhughes@utah.gov
801.538.3254

March 7, 2016

RE: CH16012 – Cloud Solutions RFP, Cover Letter

Christopher:

I am responding on behalf of Quest Media & Supplies, Inc. ("Quest Technology Management" or "Quest"), a corporation with Federal Tax Identification number 94-2838096. We are working in partnership with Pondera Solutions, Inc. ("Pondera"), a corporation with Federal Tax Identification number 45-1806211. The Quest-Pondera team accepts and is willing to comply with the requirements of this RFP and exhibits, including but not limited to Attachment A, NASPO ValuePoint Master Agreement Terms and Conditions, as negotiated, and Attachment D, Scope of Services.

We understand that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum. We comply with affirmative action and equal employment regulations.

We have not employed any company or person other than a bona fide employee working solely for Quest or Pondera to respond to this RFP. We have not paid or agreed to pay any company or person, other than a bona fide employee working solely for the Contract Vendor as our marketing agent, any fee, commission, percentage, brokerage fee, gifts or any other consideration contingent upon or resulting from the award of this contract. The Quest-Pondera team affirms its understanding and agreement that for a breach or violation of this term, the State has the right to annul the contract without liability, or in its discretion, to deduct from the contract price the amount of any such fee, commission, percentage, brokerage fee, gifts or contingencies.

The Quest team members responsible for writing this proposal are Amy Comi, Marketing, Jeff Scheel, SLED Team, and Pondera Solutions employees: Jon Coss, CEO; Caryn Otto, Business Development Manager; Tom Lucero, VP of Development; and Amanda Huston, VP of Service Delivery.

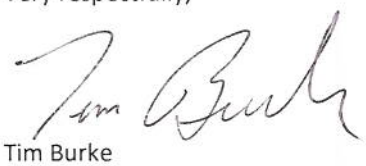
Neither Quest nor Pondera Solutions is currently suspended, debarred, or otherwise excluded from federal or state procurement and non-procurement programs. This proposal is firm and binding for one hundred eighty (180) days from the proposal opening date.

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

The Quest Pondera team intends to provide Eligible Users with a Software as a Service (SaaS) cloud service model. FDaaS is a Software as a Service private cloud service with the ability to store and secure the purchasing entity's data in the low and moderate FIPS 199 risk categories.

All costs associated for our cloud solutions have been identified in our pricing catalog.

Very respectfully,



Tim Burke
President and CEO
Quest
916.338.7070
Tim_Burke@questsys.com

Ryan O'Keeffe

Education

BACHELOR OF SCIENCE | JUNE 2008 | CALIFORNIA STATE UNIVERSITY, SACRAMENTO

- Major: Business Management

Experience

DIRECTOR, SERVICE MANAGEMENT | QUEST | 2012-PRESENT

- Work directly with leadership to review service metrics, service opportunities, and contract negotiation
- Process equipment orders based on service requirements as new services are deployed
- Work directly with vendors for new offerings to service base. Negotiate contract terms and services
- Set goals and milestones for Service Management team. Hold on-going reviews with Operation Manger
- Review market trends and future needs to meet the needs of our Clients.

OPERATIONS MANAGER, SERVICE MANAGEMENT | QUEST | 2011-2012

- Acting as the liaison between Service Managers and Operation Center management and staff; assisting with managing escalations from clients
- Evaluate each Service Manager and their effectives with their assigned accounts; report status to management
- Identify, diagnose and communicate issues with upper management
- Facilitate team meetings (recurring and ad hoc), in which you discuss Service Managers escalations or general questions

SERVICE MANAGER | QUEST | 2009-2011

- Responsible for proactively managing relationships with assigned clients, and providing the highest level of customer satisfaction for all aspects of service delivery
- Act as primary liaison between client staff and Operation Center Management and staff; managing escalations from clients
- Create, and manage detailed project plans for implementations / migrations
- Understand organizational resources, priorities, needs and policies and anticipate potential problems associated with client activity or service level trends

MANAGED SERVICES AUDITOR | QUEST | 2008-2009

- Audited Client service contract with Quest to verify services provided meet contractual needs
- Delivered weekly report to senior management on audit finds
- Worked on hardware/software vendor maintenance renewals for Managed Services department

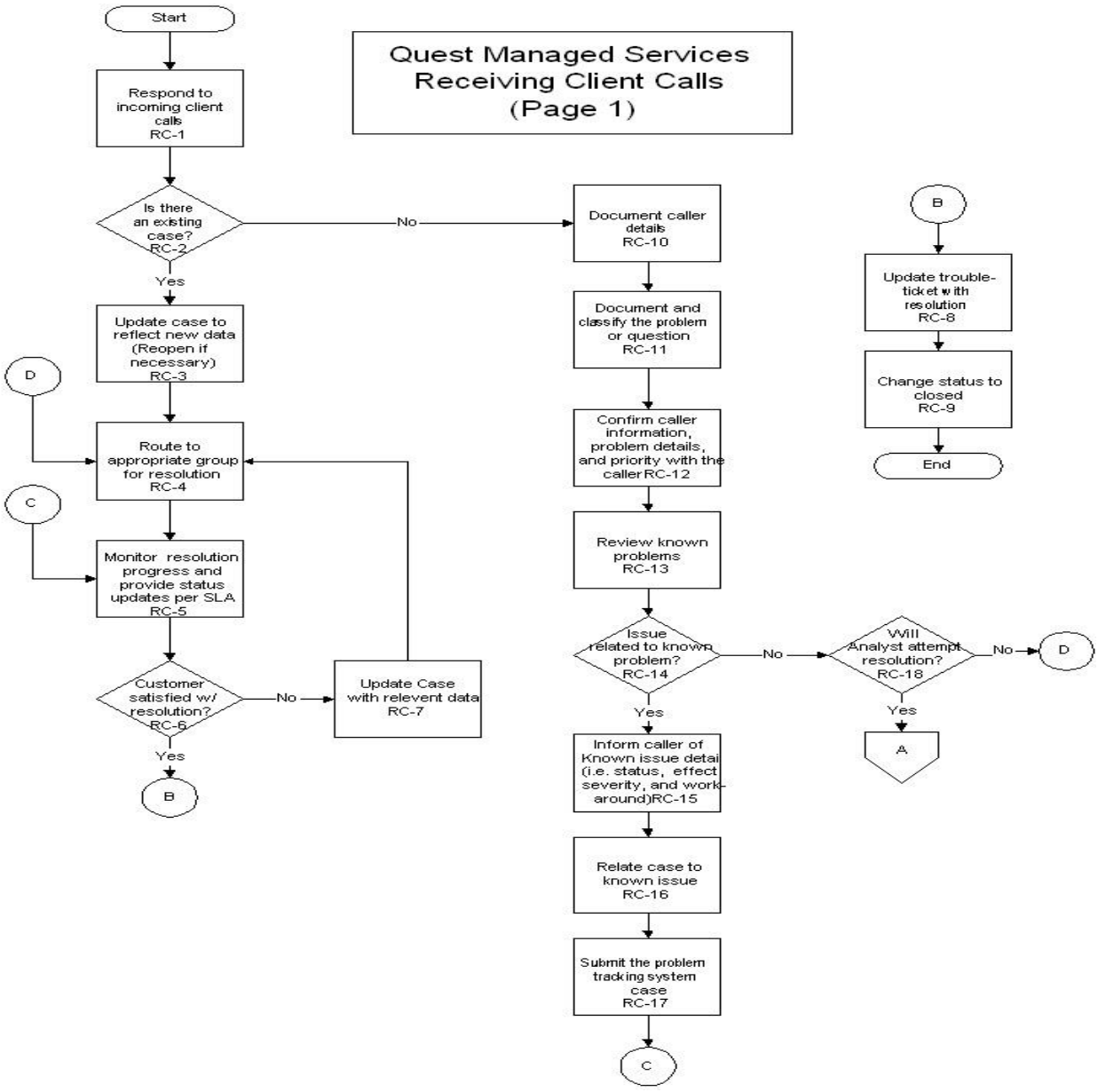
CAR PREP | ENTERPRISE RENT-A-CAR | 2004-2008

- Cleaned cars to prepare for rentals by customers.
- Reviewed rental contract with customers and checked them into their rental.

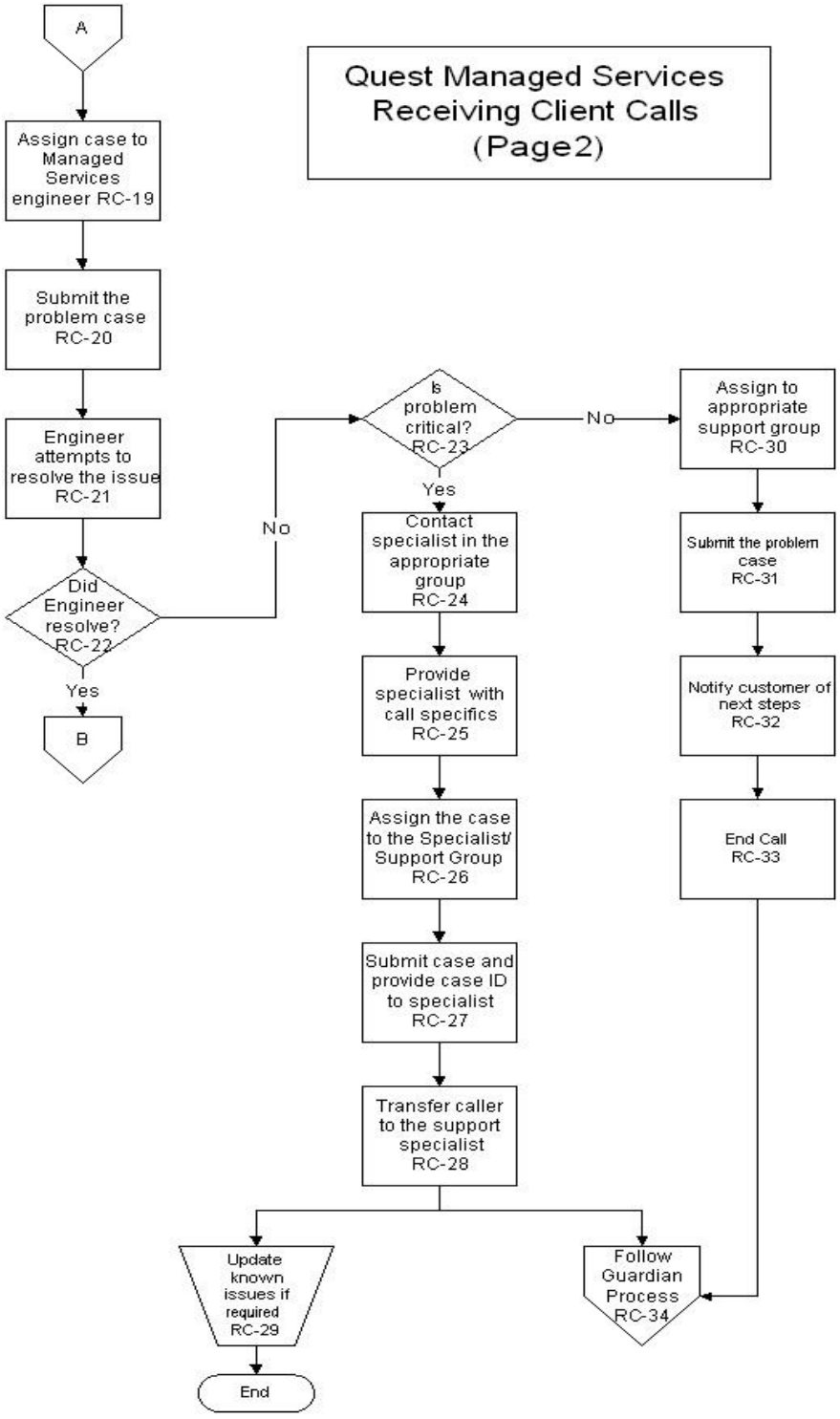
CO-OWNER | JUMPS-R-US / LEAPS-N-BOUNDS | 1998-2000

- Acquired business at age of 13
- Duties included marketing of events, financial tracking/planning, advertising, delivery, and general customer service

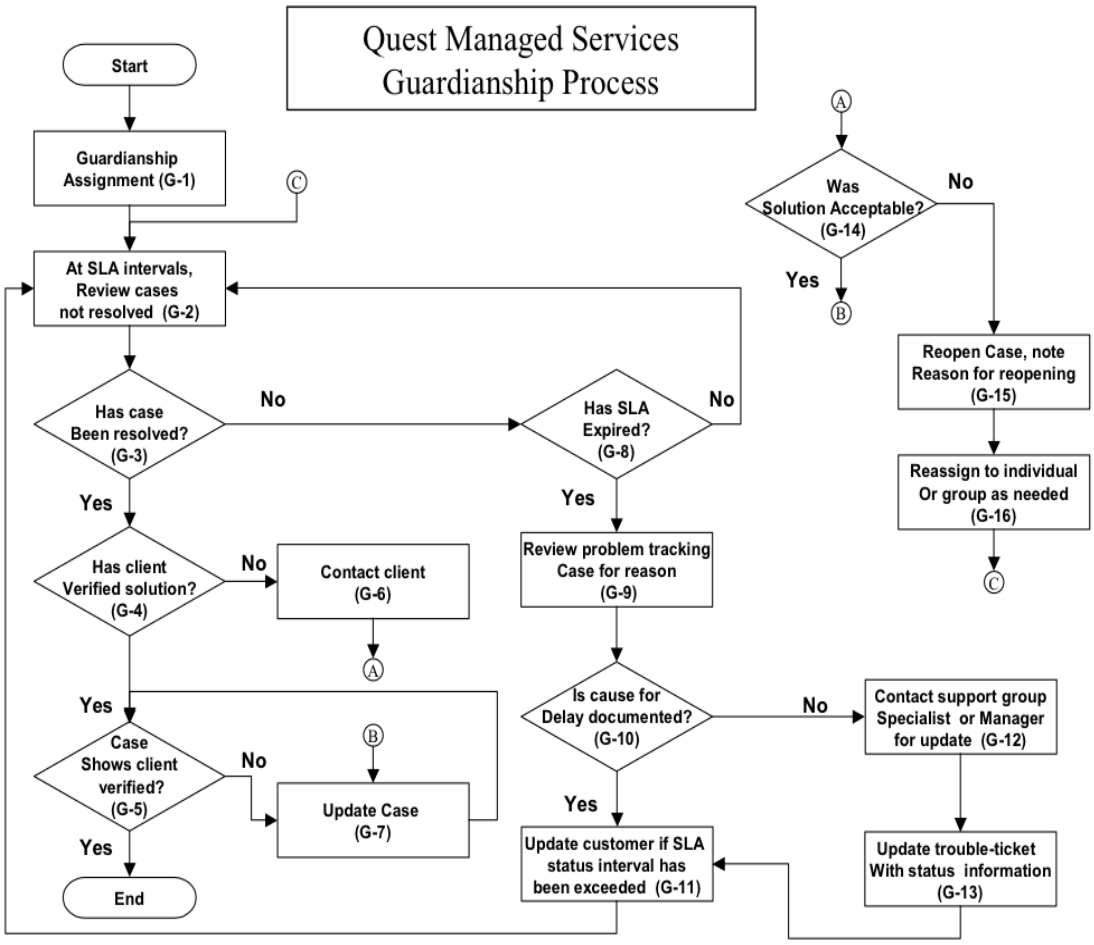
Quest Managed Services Client Call Process



Quest Managed Services Client Call Process



Quest Managed Services Client Call Process



NASPO ValuePoint FDaaS

Service Level Agreement

Quest Managed Services

Presented to:

Client Logo

Date: Month Day, Year

TABLE OF CONTENTS

INTRODUCTION

This Service Level Agreement (SLA), effective as of Month Day, Year ("effective date"), is made and entered into by and between Quest Media & Supplies Inc. (Quest), a California corporation, and _____ (Client), each referred to as a "party" and collectively as the "parties."

This SLA follows the NASPO ValuePoint Master Agreement Terms and Conditions, Attachment A and its order of precedence which is as follows:

1) A Participating Entity's Participating Addendum 1 ("PA");
2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits 2 to the Master Agreement;
3) The Solicitation;
4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
5) A Service Level Agreement issued against the Participating Addendum.

1. SERVICE SUMMARY

Quest will provide the services (quantities defined in Section 2 below) to Client. The services associated with Client's environment are as follows:

1.1. Title of Service

1.1.1. Describe Services (*include Client/Quest responsibility, expectation(s), points of clarity*)

1.2. Title of Service

1.2.1. Describe Services (*include Client/Quest responsibility, expectation(s), points of clarity*)

2. SERVICE COMPONENTS

Quest and Client have identified the following list of components (the "**services**" and collectively, the "**services package**").

Group	Components	Qty.	Services	Overage Fee	Owner of Hardware/Software
1.1	**Service Title:** Device/Component	X	Level of Service	$0.00	Quest Managed Services
1.1	**Service Title:** Device/Component	X	Level of Service	$0.00	Quest Managed Services
1.2	**Service Title:** Device/Component	X	Level of Service	$0.00	Quest Managed Services

3. MAINTENANCE, INCIDENTS, RESPONSE TIME, TICKET URGENCY LEVEL

3.1. Maintenance. A maintenance window is a defined period of time during which planned outages and changes to production services and systems may occur. The purpose of defining standard maintenance windows is to allow Client to prepare for possible disruption or changes. The following process will be utilized for the updating of services.

3.1.1. Updates/Patches. Updates will be implemented during the scheduled maintenance windows defined in the "60-day profile" described in Appendix B attached hereto. Prior to implementing any updates, Quest will send an email to Client notifying Client of the update, when it will be implemented, and its impact.

3.1.2. Changes. If configuration changes to the components are required or requested, Quest will utilize the change management process as defined in the 60-day profile. Any changes requested by Client will be completed within the requested resolution timeframe set forth in the 60-day profile and implemented during the scheduled maintenance window as defined in the 60-day profile. To request a change, Client shall send a change request in a secure manner to performance@questsys.com.

3.2. Incidents and Emergencies. If any incidents or emergencies occur, Quest will utilize the incident management process as defined in the 60-day profile. Quest will respond to and resolve all incidents within the timeframes and according to the methods set forth in the 60-day profile. To report an incident or emergency, Client shall send an incident notification in a secure manner to performance@questsys.com or by telephone to 800-443-5605.

3.3. Problem Response Time. The problem response time is the time period starting after (i) Quest's confirmation of the service event and (ii) receipt of the information required from the Client for Quest's support team to begin resolution and open a trouble ticket in Quest's systems. Due to the wide diversity of problems that can occur and the methods required to resolve them, problem response time IS NOT defined as the time between the receipt of a call and resolution of the problem. After receiving a report of fault, Quest shall use a reasonable method to provide the Client with a progress update(s).

3.4. Ticket Urgency Levels. Support, alert, or Client requests will be assigned a ticket and issued an urgency level based on priorities which are determined by request type and level of impact.

3.4.1. Low. Informational request; no issues are present or no services are impacted. For example, “What is your data center address?”

3.4.2. Med-Low. An issue or event may be impacting a single user who is able to work, or a workaround was provided. For example, “I'm unable to access questsys.com using internet explorer, but I can access it using Firefox.”

3.4.3. Medium. A monitored device is deemed non-responsive by the monitoring tool. For example, “A monitored device is reporting a “packet loss” or is inaccessible and non-responsive to triage/troubleshooting commands.”

3.4.4. Medium-High. An issue impacting the entire site, department, or multiple users for which no work around is available. For example, “The Sacramento office is unable to connect to the internet.”

3.4.5. High. An issue impacting the entire company or multiple sites for which no work around is available. For example, “No one in our company is able to get to email or make a phone call.”

4. IMPLEMENTATION AND TERM

The services, as noted in Section 1, shall be implemented, and the term under this SLA shall commence upon (i) the completion of the items listed below and (ii) the invoicing by Quest to Client of the entire Monthly Recurring Charge (MRC), as noted within Section 5. Quest may begin partial billing of the MRC as services are implemented. Partial billing of MRC does not commence the term.

4.1 Receipt by Quest of the SLA executed by Client.

4.2 Receipt by Quest of a Direct Payment Authorization from Client.

4.3 Completion of a services kick-off meeting between Quest and Client.

4.4 Receipt by Quest of a purchase order from Client (if required by Client).

4.5 Implementation of services.

5. INVESTMENT FOR SERVICES

The following table identifies Client's investment for the **service package**. Partial billing of the MRC may apply.

Quest Select Service Package	Term	Monthly Charges (MRCs)
Selected Service Package (Services listed in Section 2)	36 Months	
Setup Services	NRC	

5.1. Monthly charges may be increased to reflect changes in electrical rates by local utility companies. Quest will provide a 60-day notice of any power rate increase.

5.2. All fees are in US Dollars

5.3. Incident Response, data and/or application migration services are available upon request for an additional fee/cost.

5.4. In addition to the amounts set forth above, any technical support provided by Quest in connection with the services shall be billed by Quest on a time and materials basis pursuant to the following rate schedule.

5.4.1. Quest/Pondera Premium Technical Support Rate Schedule:

Quest/Pondera Premium Technical Support			
Item	**Description**	**List Price**	**10% Discount**
PS-PTS-OTSE	Pondera Premium Support – Onsite Technical Support Engineer	$215/hr	$193.50/hr
PS-PTS-STSE1	Pondera Premium Support – Senior Technical Support Engineer	$180/hr	$162.00/hr
PS-PTS-PTSE	Pondera Premium Support – Product Technical Support Engineer	$160/hr	$144.00/hr
PS-PTS-STSE2	Pondera Premium Support – Staff Technical Support Engineer	$140/hr	$126.00/hr
PS-PTS-ATSE	Pondera Premium Support – Associate Technical Support Engineer	$105/hr	$94.50/hr
PS-QST-MTC	Quest Remote Maintenance Services	$205/hr	$184.50/hr
PS-QST-DEP	Quest Remote Deployment Services	$185/hr	$166.50/hr
PS-QST-ADV	Quest Remote Advisory Services	$185/hr	$166.50/hr
PS-QST-SOW	Quest Remote Statement of Work Services	$185/hr	$166.50/hr
PS-QST-PRT	Quest Remote Partner Services	$185/hr	$166.50/hr
PS-QST-TDS	Quest Online Training Deployment Services	$185/hr	$166.50/hr

5.4.2. Additional Value Added Services: List price shown in table below. Discount is 10%.

Maintenance Services			**10% Discount**
Maintenance Services	Onsite Hourly Rate	$205.00	$184.50
	Remote Hourly Rate	$185.00	$166.50
Professional Services			**10% Discount**
Deployment Services	Onsite Hourly Rate	$205.00	$184.50
	Remote Hourly Rate	$185.00	$166.50
Consulting/Advisory Services	Onsite Hourly Rate	$205.00	$184.50
	Remote Hourly Rate	$185.00	$166.50
Architectural Design Services	Onsite Hourly Rate	$205.00	$184.50
	Remote Hourly Rate	$185.00	$166.50
Statement of Work Services	Onsite Hourly Rate	$205.00	$184.50
	Remote Hourly Rate	$185.00	$166.50
Partner Services			**10% Discount**
Partner Services	Onsite Hourly Rate	$205.00	$184.50
	Remote Hourly Rate	$185.00	$166.50
Training Deployment Services			**10% Discount**
Training Deployment Services	Onsite Hourly Rate	$205.00	$184.50
	Remote Hourly Rate	$185.00	$166.50

5.4.3. Emergency Incident Response Services: $385/hour with minimum amounts determined at time of incident.

5.4.3.1. Immediate response to threat

5.4.3.2. Assess your security posture against the threat

5.4.3.3. Determine the level of effort required to protect Client's assets

5.4.3.4. Work to prevent, detect and respond to incidents

5.4.3.5. Identify and mitigate complex security vulnerability

5.4.3.6. Provide risk analyses and recommendations for threat eradication

5.4.3.7. Provide forensic analysis to determine extract threat vector

5.5. Rates listed above exclude Professional Service engagement(s) and/or project(s) and are subject to rates listed in any separate engagement documents. Please contact the Quest account manager, technical consultant, or service manager for engineering rates that may fall outside of listed engineering services.

5.6. Some additional services that Quest offers, **but are not included in this SLA**, are as follows:

Services	*Optional*
Security Policy Review	✓
Server Anti-virus Protection	✓
Data Backup Services	✓
Data Encryption Services	✓
Disaster Recovery Services	✓
Firewall Policy Rule Review	✓
Security Monitoring/Management	✓
Threat Assessment	✓
Security Assessment	✓
Hardware Replacement	✓
Vulnerability Scanning	✓

6. NEW AND/OR ADDITIONAL SERVICES

6.1. The request for additional and/or new services ("new/additional services") can be made via email and/or phone call to the Quest primary points of contact. Any new/additional services added to this SLA will be documented via a separate addendum to this SLA. Services provided within subsequent addendum(s) will adhere to the terms and conditions of this SLA, unless otherwise specified within the addendum. Quest will obtain written Client approval and/or a purchase order for any new/additional services. Upon Client approval, all references to services shall include all approved new/additional services. Quest is authorized to make adjustments to the fees and surcharges charged for the services in order to cover the costs of any new/additional services. Cost and fee adjustments will be documented via email and/or a separate addendum and sent to Client prior to fee adjustment. Client agrees to pay the fees and surcharges for the services, as adjusted.

7. OVERAGE BILLING

7.1. An "overage" is defined as the usage of services provided by Quest to Client in excess of the allocated quantity, as noted within Section 2 of the SLA. Quest will assess an "overage fee"

for provided services that fall under this classification if applicable. Refer to Section 2 for overage rate information.

8. CONTRACT EXPIRATION NOTIFICATION

8.1. Client is to notify Quest thirty (30) days prior to the SLA expiration date. If Client has not notified Quest in writing of its election to extend or terminate this agreement, this SLA will automatically renew for an additional twelve (12) month term at the then current monthly/annual fees plus 10%. If Client elects to terminate the services, the termination date for the SLA will be the last day of the last month of the term. Quest does not prorate the final month's invoice.

9. TERMINATION OF THE CONTRACT

9.1. Termination for Cause.

9.1.1. If Quest fails to meet the material requirements of this SLA ("Quest Event of Default"), Client will have the right to terminate this SLA, provided that Quest has not cured such "Quest Event of Default" or Client and Quest are unable to reach agreement on remediation within thirty (30) days after the Client has notified Quest in writing of the "Quest Event of Default."

9.2. Termination for Client Default.

9.2.1. If Client shall fail to pay when due any installment of monthly fees or other amount due hereunder within ten (10) days of the date due; or Client shall fail to observe any other covenant, agreement, or requirement to be observed or performed by Client, which failure is not cured within thirty (30) days after written notice by Quest to Client (each a "Client Event of Default"), Quest shall have the right to terminate this SLA. Termination of the SLA or any services does not relieve Client of liability for all monthly charges, as identified in Section 5 of this SLA.

9.3. Termination for Insolvency, Assignment, or Material Adverse Change.

9.3.1. Either party may immediately terminate this SLA if the other party (i) becomes or is declared insolvent or bankrupt; (ii) is the subject of any proceeding related to its liquidation or insolvency (whether voluntarily or involuntarily) which is not dismissed within 90 days; (iii) makes an assignment for the benefit of creditors; or (iv)

experiences a material adverse change in financial condition which may reasonably be expected to affect its ability to pay.

9.4. Rights Upon Termination.

9.4.1. In the event that Client terminates the SLA at any time during the term of the SLA, Client agrees to pay all monthly charges as identified in Section 5 of this SLA.

9.5. Survival.

9.5.1. Articles 10, 11, 13, 14, 15, 17, and 18 shall survive any termination or expiration of this agreement.

10. OWNERSHIP OF PLACED EQUIPMENT

10.1. Client grants to Quest a limited, non-exclusive, non-transferable license to place such equipment and other materials/software necessary for Quest to provide the services under this SLA ("**Quest Materials**") on various premises owned or leased by Client at such locations as mutually agreed to by Quest and Client. This license solely grants Quest a right of use and is not intended to grant a lease, easement, or other interest in such premises.

10.2. Quest retains full ownership of the Quest Materials, and the placement of the Quest Materials on the premises does not create in Client any beneficial, equitable, leasehold, license, or other ownership right, title, or interest in the Quest Materials.

10.3. Title to the Quest Materials shall remain with Quest at all times, and Client shall protect and defend Quest's title and keep it free of all claims and liens other than those created by Quest. Client agrees to take such action at its expense as may be necessary to prevent any third party from acquiring any interest in the Quest Materials as a result of its attachment to realty.

10.4. If the Quest Materials includes or contains any software, or if any software is provided during the term of the SLA, Client agrees that it has no interest in such software and that any such software is to be used solely and exclusively in and with the Quest Materials.

10.5. Quest shall have no duty, responsibility, or obligation to make any structural alterations(s) or adjustment(s) to the premises to install the Quest Materials. Quest is not responsible for restoring Client's premises to its original condition upon removal or relocation of any or all of the Quest Materials.

10.6. During the term, Client shall furnish heat, light, and electrical power and protect the Quest Materials from theft and damage.

10.7. Subject to Client's standard administrative, safety, and security requirements and policies, Quest shall have the right at any time with no less than forty-eight (48) hours advanced notice to Client to access the premises on which any Quest Materials are located and to repair, maintain, upgrade, replace, or remove the Quest Materials.

10.8. In the event of a default by Client, or the expiration or other termination of the SLA, and subject to Client's standard administrative, safety, and security requirements and policies, Quest shall have the right to immediately access the premises on which any Quest Materials resides and remove the Quest Materials.

10.9. Client shall use commercially reasonable efforts to maintain the environment and condition of the aforementioned equipment in order that the equipment is not damaged by negligence, misuse, or abandonment.

10.10. Client agrees that Quest may from time to time file, with the appropriate filing office, a UCC-1 Financing Statement and amendments as appropriate, showing Client as the debtor, Quest as the secured party, and the Quest Materials as the collateral, solely for the purpose of providing public notice of the ownership by Quest of the Quest Materials. The filing of a UCC-1 Financing Statement by Quest covering the Quest Materials shall in no way limit the full ownership of the Quest Materials by Quest.

10.11. Client shall and does herby agree to indemnify, defend, and hold harmless Quest, and its directors, officers, employees, agents, and affiliates from any and all claims, demands, actions, suits, proceedings, costs, expenses, damages, and liabilities (including reasonable attorneys' fees) resulting from or arising out of any damage to or destruction of the Quest Materials in violation of the foregoing provisions, which obligation shall survive the expiration or termination of this agreement

11. INDEMNIFICATION

11.1. Quest 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.

11.2. Section 11.1 shall apply with respect to a disclosure of "confidential information" only to the extent such disclosure is the result of actions predominantly attributable to Quest or its subcontractors. The provisions of the paragraph survive expiration or termination of this contract.

Neither Quest nor its subcontractor of any tier shall be held liable under these sections (11.1 and 11.2) for more than $10,000.00 or as defined in the limitation of liability section (paragraph Limitation of Amount of Liability), whichever is less.

12. BILLING TERMS

12.1. Costs for the services will be billed and paid at the beginning of each month by Client through an automatic clearing house (**ACH**) process. Schedule A must be completed and returned to Quest prior to the first month of billing under this SLA.

12.2. Payments returned for non-sufficient funds, stop payment requests, or a closed account will result in a collection fee of $75.00 for the first offense plus the amount to be collected. Subsequent offenses will result in a $225 returned payment fee, per offense, plus the amount to be collected thereafter.

12.3. Charges for technical support as set forth on repair ticket requests from Client will be invoiced by Quest once per month and are due and payable by Client within ten (10) days of invoice date. All payments are due upon receipt of invoice. Payments received later than ten (10) days after invoice shall accrue interest at 10% per annum. Client agrees that any late or missed payment is a material breach of this SLA.

12.4. All payments to Quest shall be net of all taxes, charges, and other fees. Client shall be solely liable for and shall pay any state or local tax, fee, charge, or surcharge payable for services that are subject to such imposition.

13. CONFIDENTIALITY

13.1. Quest agrees that Quest and its agents and personnel may have access to confidential and proprietary information and materials belonging to or disclosed by Client, whether disclosed electronically, orally, in writing, or by display, which are not generally disclosed to or known by the public, concerning or pertaining to the business of Client, including, without limitation, trade secrets, data, reports, methods, techniques, procedures, processes, methodologies, forecast, plans, employee information, and Client information, and that such information is commercially valuable to Client or is otherwise confidential and proprietary to Client ("confidential information"). Confidential information shall not include any information to the extent that it (i) is or becomes a part of the public domain through no act or omission on the part of Quest; (ii) is disclosed to third parties by Client without restriction on such third parties: (iii) is in Quest's possession, without actual or constructive knowledge of an obligation of confidentiality with respect thereto, at or prior to the time of disclosure under this SLA; (iv) is disclosed to Quest by a third party; (v) is independently developed by Quest without reference to the disclosing party's confidential information; or (vi) is released from confidential treatment by written consent of Client. Quest agrees that nothing in this SLA grants to it any license, right, title, or interest in or to the confidential information, except as expressly set forth herein. Client reserves all rights to its confidential information not expressly granted in this SLA. Quest agrees to use confidential information solely for the purposes of this SLA and pursuant to the terms of this SLA and for no other purpose whatsoever. Quest agrees to hold such information in the strictest confidence. Quest shall use reasonable efforts to protect the confidentiality of Client's confidential information, treating it as Quest would its own confidential information of a similar nature and value. Quest agrees to provide Client with such further assurances as reasonably requested by Client from time to time.

14. NON-SOLICITATION

14.1. **Quest.** During the term and for a period of one (1) year thereafter, Quest agrees not to hire, solicit, or attempt to solicit the services of any employee or subcontractor of Client without the prior written consent of Client. Violation of this provision shall entitle Client to assert

liquidated damages against Quest equal to one (1) year of billable engineering time or $50,000.00, whichever is greater.

14.2. Client. During the term and for a period of one (1) year thereafter, Client agrees not to hire, solicit, or attempt to solicit the services of any employee or subcontractor of Quest without the prior written consent of Quest. Violation of this provision shall entitle Quest to assert liquidated damages against Client equal to one (1) year of billable engineering time or $50,000.00, whichever is greater.

15. INDEPENDENT CONTRACTOR STATUS

15.1. Parties agree that Quest is an independent contractor providing professional services and not an employee, agent, joint venture, or partner of Client. Nothing in this SLA, nor in a course of dealing between the parties, shall be interpreted or construed as creating the relationship of employer and employee, principal and agent, joint ventures, or partners between Quest and Client and/or its personnel. Neither party shall have any right, power, or authority, expressed or implied, to bind the other.

16. INSURANCE

16.1. Required Coverage. During the term, each party shall obtain and maintain at each party's sole cost and expense the following:

a. Standard form personal property insurance insuring all equipment, alterations, fixtures, and personal property of any kind for which Client, the covered party, is legally liable or which the covered party has had installed at or around the other party's facility, for fire, extended coverage for vandalism, malicious mischief, and special extended/all-risk coverage for sprinkler leakage. Such insurance shall be in an amount no less than 100% of the full replacement cost thereof.

b. Commercial general liability insurance insuring the covered party against any and all claims for bodily injury and property damage arising out of this agreement and the covered party's use, occupancy, and/or maintenance of any of the other party's facilities. Such insurance shall have a combined single limit of no less than $1,000,000.00 per occurrence, with no less than a $3,000,000.00 aggregate limit. The policy shall list the other party as an additional insured (not including any commercial auto liability). In no

event shall the bounds of such insurance limit the liability of either party under this agreement.

16.2. Certificate of Insurance. A commercially acceptable certificate of insurance shall be delivered by the covered party to the other party prior to the commencement date of this SLA and annually thereafter at least 30 days prior to the expiration date of the original policy or any renewal thereof.

17. LIMITATION OF LIABILITY

17.1. In no case shall Quest's maximum liability arising out of this SLA, whether based upon warranty, contract, negligence, tort, strict liability, or otherwise, exceed in the aggregate, the actual payments received by Quest under this SLA during the six (6) months immediately prior to the event giving rise to the claim.

17.2. In no event shall either party be liable for indirect, special, incidental, or consequential damages, including, but not limited to, loss of profits, loss of revenues, loss of opportunities, loss of data, or loss of use damages, arising out of this agreement, even if the party has been advised of the possibility of such damages.

18. GENERAL TERMS

18.1. Notices. Any notice under this SLA shall be in writing, and any written notice or other document shall be deemed to have been duly given (i) on the date of personal service on the parties; (ii) two days after deposit in the United States Mail, certified or registered mail, return receipt requested, postage prepaid; (iii) one day after being sent by professional or overnight courier or messenger service guaranteeing one day delivery, with receipt confirmed by the courier; or (iv) on the date of transmission if sent by facsimile, telegram, telex, telecopy, or other means of electronic transmission resulting in written copies, with receipt confirmed. Unless otherwise provided in writing, any such notice shall be delivered or addressed to the parties as follows.

If to Quest: 5822 Roseville Road, Sacramento, CA 95842

If to Client:

18.2. Failure to conform to the requirement that mailings be done by registered or certified mail shall not defeat the effectiveness of notice actually received by the addressee.

18.3. Entire Agreement. This document, with all exhibits, schedules and addenda, constitutes the entire agreement between the parties, all oral agreements being merged in this document, and supersedes all prior representations. There are no representations, agreements, arrangements, or understandings, oral or written, between or among the parties relating to the subject matter of this SLA that are not fully expressed herein.

18.4. Assignability. This SLA shall not be assigned by either party without the prior written consent of the other party.

18.5. Waiver. Any of the terms or conditions of this SLA may be waived at any time by the party entitled to the benefit thereof, but no such waiver shall affect or impair the right of the waiving party to require observance, performance, or satisfaction of that term or condition as it applies on a subsequent occasion or of any other term or condition hereof.

18.6. Amendment. The provisions of this SLA may be modified at any time by agreement of the parties. Any such agreement hereafter made shall be ineffective to modify this SLA in any respect unless in writing and signed by the parties against whom enforcement of the modification or discharge is sought.

18.7. Severability. If any provision of this SLA is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of this SLA which can be given effect without the invalid provision shall continue in full force and effect and shall in no way be impaired or invalidated.

18.8. Attorneys' Fees. In the event that any party to this SLA files any petition or institutes litigation, including arbitration, to interpret or enforce the terms of this SLA, the parties expressly agree that the prevailing party or parties, in addition to any other relief provided by law, will be entitled to such reasonable attorneys' fees and court costs as may be incurred.

18.9. Jurisdiction and Venue. Any legal proceeding by a party to enforce any provision of this SLA or arising out of this SLA must be brought in the California Superior Court in the County of Sacramento or the United States Court for the Eastern District of California, as applicable, and each party consents to the jurisdiction of such courts and waives any objection to the

venue laid therein. Client and Quest hereby unconditionally and irrevocably waive the right to a jury trial of any claim or cause of action between the parties directly or indirectly relating to this SLA or the subject matter hereof, any services schedule or the subject matter thereof, or any equipment. This SLA may be filed as a written consent to a trial without jury by any court.

18.10. Binding Effect. The parties expressly agree that this SLA is binding on each other's successors, heirs, assigns, beneficiaries, executors, administrators, and trustees.

18.11. Governing Law and Venue. The rights and obligations of the parties and the interpretation and performance of this SLA shall be governed by the laws of the Participating Entity's or Purchasing Entity's 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.

18.11.1. 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.

18.11.2. 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.

18.11.3. 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.

18.12. Parties in Interest. Nothing in this SLA, explicit or implied, is intended to confer any rights or remedies under or by reason of this SLA on any persons other than the parties to it and their respective successors and assigns, nor is anything in this SLA intended to relieve or discharge

the obligation or liability of any third person to any party to this SLA, nor shall any provision give any third person any right of subrogation or action against any party to this SLA.

18.13. Captions. All paragraph captions are for reference only and shall not be considered in construing this agreement.

18.14. Construction. This SLA shall not be construed against any party; instead, it shall be construed as though all parties have participated in its drafting. No promises or inducements have been made to the parties to this SLA. This SLA is entered into freely and voluntarily.

18.15. Counterparts. This SLA may be executed in counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same document.

Each of the authorized parties has executed this SLA as of the effective date.

CLIENT:		**QUEST:**	
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____
Contract/PO#:	_____		

Quest Account Manager:

Name:

Email:

Mail: 5822 Roseville Rd., Sacramento, CA 95842

Phone: (916) 338-7070

Quest Technical Consultant:

Name:

Email:

Mail: 5822 Roseville Rd., Sacramento, CA 95842

Phone: (916) 338-7070

Client Representative:

Name:

Email:

Mail:

Phone:

Authorized Contract Signer - Client:

Name:

Email:

Mail:

Phone:

Quest is an equal opportunity employer with affirmative action obligations, meaning it actively seeks qualified job candidates who are minorities, women, disabled, and protected veterans. By accepting this contract or purchase order, you also accept any responsibility for abiding by all the regulatory requirements at **41 CFR 60-2, 41 CFR 60-300 and 41 CFR 60-741**. These regulations prohibit discrimination against minorities, women, qualified individuals with disabilities, and qualified protected veterans and requires affirmative action by covered prime contractors and subcontractors for the employment and advancement in employment of qualified protected veterans. Those requirements are incorporated here for reference.

APPENDIX A – DATA CENTER FACILITY STANDARDS AND WARRANTY

Force Majeure Event: any act of God, fire, casualty, flood, war, terrorism, strike, lock out, failure of public utilities, injunction or any act, exercise, assertion or requirement of any governmental authority, epidemic, public health emergency, destruction of production facilities, insurrection, inability to obtain labor, materials, equipment, transportation or energy sufficient to meet needs, or any other cause beyond the reasonable control of a party.

Service Interruption: a complete loss of signal that renders the services unusable.

Planned Service Interruption: any service interruption caused by planned work such as scheduled maintenance or planned enhancements or upgrades.

During the term of this SLA, Quest warrants that (i) the services will be available 99.9% of the time per calendar month and (ii) if the services are not available, with the exception of services impacted by Internet performance or availability, Quest's liability for any service interruption (individually or collectively, "liability"), shall be limited to the amounts set forth in Table 1 below. For the purposes of calculating credit for any such liability, the liability period begins when Client reports an interruption in any portion of the service to Quest, provided that the liability shall be deemed resolved upon the closing of the same trouble ticket or the termination of the interruption, if sooner, less any time Quest is awaiting additional information or premises testing from Client. In no event shall the total amount of credit issued to Client's account on a per-month basis exceed 50% of the total monthly charges. Service interruptions will not be aggregated for purposes of determining credit allowances. To qualify, Client must request the credit from Quest within 30 days of the interruption. Client will not be entitled to any additional credits for service interruptions. Quest shall not be liable for any liability caused by force majeure events, planned service interruptions (as set forth in Appendix B), or as a result of Client's acts, omissions, or equipment. Service credits will not entitle Client to any refund or other payment from Quest. Service credits may not be transferred or applied to any other account.

THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE CONCERNING MERCHANTABILITY, TITLE, OR FITNESS FOR A PARTICULAR PURPOSE, AND NO REPRESENTATION OR STATEMENT NOT EXPRESSLY CONTAINED IN THIS SLA WILL BE BINDING ON THE CONSULTANT AS A WARRANTY. THIS APPENDIX A STATES THE ENTIRE LIABILITY OF QUEST AND THE EXCLUSIVE REMEDY OF CLIENT WITH RESPECT TO QUEST'S BREACH OF ANY WARRANTY HEREUNDER.

Table 1

Length of Service Interruption	Amount of Credit
< 40 minutes	None
40 minutes – 4 hours	5% of total Monthly Charges
4 hours – 8 hours	10% of total Monthly Charges
8 hours – 12 hours	20% of total Monthly Charges
12 hours – 16 hours	30% of total Monthly Charges
16 hours – 24 hours	40% of total Monthly Charges
24 hours or greater	50% of total Monthly Charges
THE TOTAL CREDIT ALLOWANCES PER MONTH ARE CAPPED AT 50% OF THAT MONTH'S MONTHLY CHARGES FOR THE INTERRUPTED SERVICE. SERVICE INTERRUPTIONS ARE NOT AGGREGATED FOR THE PURPOSES OF DETERMINING CREDIT ALLOWANCES.	

APPENDIX B - INITIAL 60-DAY PROFILE

Quest and Client will develop an initial 60 Day Profile to reference the following:

- Incident Management Procedures
- Maintenance Schedule and Procedure
- Service Changes
- Service Updates
- Escalation Authority List
- Client Component List (Appendix C)
- Notification List/Contact List
- Ticket Urgency Matrix

APPENDIX C - CLIENT COMPONENT LIST

To be completed as part of the 60 day profile

APPENDIX D - NEW/ADDITIONAL SERVICES AND PRICING

Insert Client worksheet here.

SCHEDULE A TO SERVICE LEVEL AGREEMENT

Authorization Agreement for Direct Payments (ACH Debits)

As a condition to Quest entering into the attached Service Level Agreement, Client hereby enters into this Authorization Agreement for Direct Payments. By executing this Authorization Agreement for Direct Payments, the undersigned hereby authorizes Quest to initiate debit entries to the account identified below ("account") at the Depository Financial Institution identified below ("DFI") and debit the same to the account for any advance payment(s), installation fee(s), or monthly service fee(s) required by the Service Level Agreement.

The undersigned further represents and warrants that (i) the undersigned is a duly authorized representative of Client; (ii) the account is a business account and is not an account used for personal or household purposes; and (iii) if the account is closed for any reason whatsoever, Client will enter into a new Authorization Agreement for Direct Payments with respect to a replacement account within five (5) business days of the closing of the account identified herein.

Name of DFI			
DFI's Routing Number *(9 digits only)*			
Account Number			
Branch	City	State	Zip

This authorization will remain in full force and effect until Client provides Quest with written notification of Client's termination of this Authorization Agreement for Direct Payments in such time and in such manner as to afford Quest and DFI a reasonable opportunity to act upon such termination.

Signature of Duly Authorized Representative of Client	Date
Company Name:	
Phone Number	Federal Tax Identification Number

**** Please attach voided check to this authorization****

Important Notification About ACH Debits

Quest will automatically debit the account for periodic applicable payments as set forth above. Quest will invoice Client directly until the ACH debits are implemented as set forth in the lease agreement. Client must remit all invoices received from Quest by their respective due date. Once ACH debits are implemented, Client will continue to receive invoices from Quest that will be labeled as "For Notification Purposes Only. We will automatically draft your account for the amount detailed below [.]"

Client (initial): _____