STATE OF VERMONT PARTICIPATING ADDENDUM # 38001
FOR NASPO VALUEPOINT PURCHASING PROGRAM: CLOUD SOLUTIONS
Led by the State of Utah
Master Agreement #AR2504

Contractor: GuideSoft, Inc. dba Knowledge Services

Contractor's NASPO ValuePoint Webpage: https://www.naspovaluepoint.org/portfolios/portfolio-contractor/knowledge-services-cloud-solutions/

1. ***Parties.*** This Participating Addendum is a contract between the State of Vermont, through its Department of Buildings and General Services, Office of Purchasing & Contracting (hereinafter "State" or "Vermont"), and the Contractor identified above. It is the Contractor's responsibility to contact the Vermont Department of Taxes to determine if, by law, the Contractor is required to have a Vermont Department of Taxes Business Account Number.

2. ***Subject Matter.*** This Participating Addendum authorizes the purchase of Cloud Solutions from Contractor pursuant to the Master Agreement identified above, which is hereby incorporated by reference. Contractor's awarded categories are:

    a. **Software as a Service (SaaS):** As used in this Participation Addendum 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.

3. ***Definitions.*** Capitalized terms used, but not defined herein, have the meanings ascribed to such terms in the Master Agreement between the Lead State and the Contractor.

4. ***Purchasing Entities.*** This Participating Addendum may be used by (a) all departments, offices, institutions, and other agencies of the State of Vermont and counties (each a "State Purchaser") according to the process for ordering and other restrictions applicable to State Purchasers set forth herein; and (b) political subdivisions of the State of Vermont and any institution of higher education chartered in Vermont and accredited or holding a certificate of approval from the State Board of Education as authorized under 29 V.S.A. § 902 (each an "Additional Purchaser"). Issues concerning interpretation and eligibility for participation are solely within the authority of the State of Vermont Chief Procurement Officer. The State of Vermont and its officers and employees shall have no responsibility or liability for Additional Purchasers. Each Additional Purchaser is to make its own determination whether this Participating Addendum and the Master Agreement are consistent with its procurement policies and regulations.

5. ***Contract Term.*** The period of Contractor's performance shall begin on May 15, 2019 and end upon expiration of the Master Agreement, unless terminated earlier in accordance with the terms of this Participating Addendum or the Master Agreement. An amendment to this Participating Addendum shall not be necessary in the event of the renewal or extension of the Master Agreement.

6. ***Available Products and Services.*** All products, services and accessories listed on the Contractor's NASPO ValuePoint Webpage may be purchased under this Participating Addendum.

7. ***No Lease Agreements*.** Contractor is prohibited from leasing to State Purchasers under this Participating Addendum. Additional Purchasers are not subject to this prohibition and may negotiate lease agreements with Contractor if the terms of the Master Agreement permit leasing.

8. ***Requirements for Ordering.***

    a. Orders made under this Participating Addendum must include a specifically-negotiated Statement of Work or Service Level Agreement terms as necessary for the Product and/or Service to meet the Purchasing Entity's requirements. Orders funded by federal funds may include additional terms as necessary to comply with federal requirements.

        i. Prior to entering into Statement of Work or Service Level Agreement with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and/or Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

    b. State Purchasers must follow the ordering procedures of the State Contract Administrator to execute orders against this Participating Addendum, which shall include, as applicable, obtaining approval from the State CIO and/or Attorney General's Office prior to making purchases under this Participating Addendum.

    c. The State's Agency of Digital Services Procurement Office is the only entity authorized to place orders on behalf of State Purchasers. Contractor agrees that it will not accept or fulfill orders placed on behalf of State Purchasers from any other source. Contractor's failure to meet this requirement may result in suspension or termination of this Participating Addendum.

    d. All orders placed under this Participating Addendum must include the Participating Addendum Number on the Purchase Order.

9. ***Payment Provisions and Invoicing.***

    a. Product offerings and complete details of product pricing, including discounts, applicable to this Participating Addendum are set forth in the Price Schedule maintained on-line at Contractor's NASPO ValuePoint Webpage listed above.

    b. Purchasing Entities may solicit the Contractor or Fulfillment Partner/Authorized Reseller for deeper discounts than the minimum contract pricing as set forth in the Price Schedule (e.g., additional volume pricing, incremental discounts, firm fixed pricing or other incentives).

    c. If applicable, all equipment pricing is to include F.O.B. delivery to the ordering facility. No request for extra delivery cost will be honored.

    d. In the discretion of the Purchasing Entity, retainage may be specified in a Purchase Order, in an amount mutually agreeable to the parties.

    e. Payment terms are Net 30 days from the date the State receives an error-free invoice with all necessary and complete supporting documentation. Invoices shall itemize all work performed during the invoice period, including, as applicable, the dates of service, rates of pay, hours of work performed, and any other information and/or documentation appropriate and sufficient

to substantiate the amount invoiced for payment. As applicable, a copy of the notice(s) of acceptance shall accompany invoices submitted for payment.

f. Invoices shall be sent to the address identified on the Purchasing Entity's Purchase Order and shall specify the address to which payments will be sent. The State of Vermont Participating Addendum Number and Purchasing Entity's Purchase Order Number shall appear on each invoice for all purchases placed under this Participating Addendum.

g. Reimbursement of expenses is not authorized. All rates set forth in a Purchase Order shall be inclusive of any and all Contractor fees and expenses.

h. Unopened Products can be returned with no restocking fee up to 30 days from the date of receipt.

i. The State Purchasing Card may be used by State Purchasers for the payment of invoices. Use of the Purchasing Card requires all required documentation applicable to the purchase. The Purchasing Card is a payment mechanism, not a procurement approach and, therefore, does not relieve State Purchasers from adhering to all procurement laws, regulations, policies, procedures, and best practices.

10. ***Fulfillment Partners/Authorized Resellers.***

a. Resellers (or Fulfillment Partners) are available for this Participating Addendum if and to the extent approved by the State Chief Procurement Officer (each an "Authorized Reseller"). Any Authorized Resellers will be listed on the Contractor's NASPO ValuePoint Webpage listed above.

   i. The State does not intend to approve resellers or fulfilment partners for this Participating Addendum except as required to provide services for certain Products (e.g., where a Product requires a managed service provider or other such services that Contractor is unable to provide without engaging a third party). Contractor shall notify the State when a Product requested by a Vermont Purchasing Entity will require engagement of a third party. The State Chief Procurement Officer may, in its discretion, approve the third-party engagement on a limited basis, for the specific purchase only, or on a general basis, for whenever such Product is purchased under this Participating Addendum.

   ii. A reseller or fulfilment partner approved by the State for this Participating Addendum is expressly not authorized to invoice State Purchasers directly. This provision shall not apply to Additional Purchasers.

b. All State policies, guidelines and requirements shall apply to Authorized Resellers.

c. Contractor shall be responsible for successful performance and compliance with all requirements in accordance with the terms and conditions set forth by this Participating Addendum. Contractor acknowledges that each and all of the promises it makes as "Contractor" in the Master Agreement and in this Participating Addendum will apply to all Products and Services provided hereunder, regardless of who is providing or licensing the Product or performing the work.

i. Contractor promises that Purchasing Entities will not be required to affirmatively accept additional terms and conditions to use or access any Product or Service purchased under this Participating Addendum, whether by electronic means (e.g., click-through) or otherwise.

ii. Contractor promises that each of the third parties whose Products and/or Services are available for purchase under this Participating Addendum understand and agree that the terms and conditions applicable to their Products and/or Services are as set forth in the Master Agreement, as amended, and are subordinate to the terms of this Participating Addendum and the NASPO ValuePoint Master Agreement Terms & Conditions and associated service model Exhibits.

11. ***Reporting.*** Contractor shall submit quarterly reports electronically in the same format as set forth under the Master Agreement, detailing the purchasing of all items under this Participating Addendum. Contractor's reporting shall state "no activity" for any month in which there is no activity during a quarterly reporting period.

    a. The reports shall be an excel spreadsheet transmitted electronically to SOV.ThePathForward@vermont.gov.

    b. Reports are due for each quarter as follows:

Reporting Period	Report Due
January 1 to March 31	April 30
April 1 to June 30	July 31
July 1 to September 30	October 31
October 1 to December 31	January 31

    c. Failure to meet these reporting requirements may result in suspension or termination of this Participating Addendum.

12. ***Prior Approvals.*** In accordance with current State law, bulletins, and interpretations, this Participating Addendum shall not be binding until it has been approved by the Vermont Attorney General's Office, the Secretary of Administration, and the State's Chief Information Officer.

13. ***Amendment.*** No changes, modifications, or amendments in the terms and conditions of this Participating Addendum shall be effective unless reduced to writing, numbered and signed by the duly authorized representative of the State and Contractor.

14. ***Termination.*** This Participating Addendum may be terminated by the State at any time upon 30 days prior written notice to the Contractor. Upon termination or expiration of this Participating Addendum, each party will assist the other in orderly termination of the Participating Addendum and the transfer of all assets, tangible and intangible, as may facilitate the orderly, non-disrupted business continuation of each party. This provision shall not relieve the Contractor of the obligation to perform under any order executed prior to the effective date of termination or other expiration of this Participating Addendum.

15. ***Primary Contacts***. The Parties will keep and maintain current at all times a primary point of contact for this Participating Addendum. The primary contacts for this this Participating Addendum are as follows:

    a. ***For the Contractor***:

Name:	Cindy Davis
Phone:	317/806-6104
Email:	CindyD@knowledgeservices.com

    b. ***For the State***:

Name:	State of Vermont, Stephen Fazekas
Address:	109 State Street, Montpelier, VT 05633-3001
Phone:	802/828-2210
Fax:	802/828-2222
Email:	Stephen.fazekas@vermont.gov

16. Additional Terms and Conditions.

a. Notwithstanding any contrary language anywhere, in no event shall the terms of this contract or any document furnished by Contractor in connection with performance under this contract obligate the State to (1) defend or indemnify Contractor or any third party, or (2) otherwise be liable for the expenses or reimbursement, including attorneys' fees, collection costs or other costs of Contractor or any third party.

b. If required by an order made by a State Purchaser under this Participating Addendum, the terms and conditions of the State of Vermont Business Associate Agreement, revised July 7, 2017 (the six-page document available online at: https://bgs.vermont.gov/sites/bgs/files/files/purchasing-contracting/contracts/Attachment_E_BAA_HIPAA_071717REV.doc) shall be incorporated by reference and apply to the order. This provision shall not apply to Additional Purchasers.

c. Contractor is required at all times to comply with all applicable federal and state laws and regulations pertaining to information security and privacy.

d. **Governing Law, Jurisdiction and Venue; No Waiver of Jury Trial:** This Agreement will be governed by the laws of the State of Vermont. Any action or proceeding brought by either the State or the Contractor in connection with this Agreement shall be brought and enforced in the Superior Court of the State of Vermont, Civil Division, Washington Unit. Contractor irrevocably submits to the jurisdiction of this court for any action or proceeding regarding this Agreement. Contractor agrees that it must first exhaust any applicable administrative remedies with respect to any cause of action that it may have against the State with regard to its performance under this Agreement. Contractor agrees that the State shall not be required to submit to binding arbitration or waive its right to a jury trial.

e. **Sovereign Immunity:** The State reserves all immunities, defenses, rights or actions arising out of the State's sovereign status or under the Eleventh Amendment to the United States Constitution. No waiver of the State's immunities, defenses, rights or actions shall be implied or otherwise deemed to exist by reason of the State's entry into this Agreement.

f. **False Claims Act:** Contractor acknowledges that it is subject to the Vermont False Claims Act as set forth in 32 V.S.A. § 630 *et seq.* Contractor's liability to the State under the False Claims Act shall not be limited notwithstanding any agreement of the State to otherwise limit Contractor's liability.

g. **Whistleblower Protections:** Contractor shall not discriminate or retaliate against one of its employees or agents for disclosing information concerning a violation of law, fraud, waste, abuse of authority or acts threatening health or safety, including but not limited to allegations concerning the False Claims Act. Further, Contractor shall not require such employees or agents to forego monetary awards as a result of such disclosures, nor should they be required to report misconduct to Contractor or its agents prior to reporting to any governmental entity and/or the public.

h. **Fair Employment Practices and Americans with Disabilities Act:** Contractor agrees to comply with the requirement of 21 V.S.A. Chapter 5, Subchapter 6, relating to fair employment practices, to the full extent applicable. Contractor shall also ensure, to the full extent required by the Americans with Disabilities Act of 1990, as amended, that qualified individuals with disabilities receive equitable access to the services, programs, and activities provided by Contractor under this Agreement.

i. **Set Off:** The State may set off any sums which Contractor owes the State against any sums due Contractor under this Agreement; provided, however, that any set off of amounts due the State of Vermont as taxes shall be in accordance with the procedures set forth in 32 V.S.A. § 3113.

j. **Taxes Due to the State:** Contractor certifies under the pains and penalties of perjury that, as of the date this Agreement is signed, Contractor is in good standing with respect to, or in full compliance with, a plan to pay any and all taxes due the State of Vermont.

k. **Taxation of Purchases:** All State purchases must be invoiced tax free. An exemption certificate will be furnished upon request with respect to otherwise taxable items.

l. **Certification Regarding Debarment:** Contractor certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, neither Contractor nor Contractor's principals (officers, directors, owners, or partners) are presently debarred, suspended, proposed for debarment, declared ineligible or excluded from participation in Federal programs, or programs supported in whole or in part by Federal funds. Contractor further certifies under pains and penalties of perjury that, as of the date that this Agreement is signed, Contractor is not presently debarred, suspended, nor named on the State's debarment list at: http://bgs.vermont.gov/purchasing/debarment

m. **Confidentiality:** Contractor acknowledges and agrees that this Agreement and any and all information obtained by the State from the Party in connection with this Agreement are subject to the State of Vermont Access to Public Records Act, 1 V.S.A. § 315 et seq.

n. **Marketing:** Contractor shall not refer to the State in any publicity materials, information pamphlets, press releases, research reports, advertising, sales promotions, trade shows, or marketing materials or similar communications to third parties except with the prior written consent of the State.

o. **Non-Appropriation:** If an order made under this Participating Addendum extends into more than one fiscal year of the State (July 1 to June 30), and if appropriations are insufficient to support the order, the State Purchaser may cancel the order at the end of the fiscal year, or otherwise upon the expiration of existing appropriation authority. If the order is funded in whole or in part by Federal funds, and those Federal funds become unavailable or reduced, the State Purchaser may suspend or cancel the order immediately and shall have no obligation to pay from State revenues.

p. **Continuity of Performance:** In the event of a dispute between Contractor and the State, each party will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.

q. **State Facilities:** If the State makes space available to Contractor in any State facility during the term of this Agreement for purposes of Contractor's performance under this Agreement, Contractor shall only use the space in accordance with all policies and procedures governing access to and use of State facilities which shall be made available upon request. State facilities will be made available to Party on an "AS IS, WHERE IS" basis, with no warranties whatsoever.

r. **SOV Cybersecurity Standard 19-01:** All products and service provided to or for the use of the State under this Contract shall be in compliance with State of Vermont Cybersecurity Standard 19-01, which Contractor acknowledges has been provided to it, and is available on-line at the following URL: https://digitalservices.vermont.gov/cybersecurity/cybersecurity-standards-and-directives

By signing below Contractor agrees to offer the products and services on the Master Agreement at prices equal to or lower than the prices listed on the Master Agreement.

WE THE UNDERSIGNED PARTIES AGREE TO BE BOUND BY THIS CONTRACT

By the State of Vermont:

Date: _____

Signature: _____

Name: _____

Title: _____

By GuideSoft, Inc. dba Knowledge Services:

Date: _____

Signature: _____

Name: _____

Title: _____

Contract # AR2504

STATE OF UTAH COOPERATIVE CONTRACT

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

GuideSoft, Inc. dba Knowledge Services
Name

5875 Castle Creek Parkway N Drive, Suite 400
Address

Indianapolis IN 46250
City State Zip

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

Contact Person Cindy Davis Phone #(317) 806-6104 Email CindyD@knowledgeservices.com
Vendor #VC0000191176 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. Payment: Prompt Payment Discount (if any): N/A.

6. 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.

7. 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: dotStaff Terms of Use, Mobile Case Mangement Solution, and SLAs
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

Katie Belange 10/11/2016
Contractor's signature Date

Katie Belange, corporate counsel
Type or Print Name and Title

STATE

for Director, Division of Purchasing 10.17.16
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 – Scope of Services

The service and deployment model that Knowledge Services is capable of providing under the terms of the Master Agreement is Software as a Service and the deployment model is Private Cloud. Knowledge Services is capable of storing and securing low and moderate risk data.

knowledge services

Cost Proposal:
Cloud Solutions

Utah Solicitation No. CH16012
In conjunction with NASPO ValuePoint

Opening Date and Time:
Thursday, March 10, 2016, 1:00 p.m. MTN

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

Attachment G – Cost Schedule

Attachment G – 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 %** 12.5%
Infrastructure as a Service	**Discount %** _____
Platform as a Services	**Discount %** _____
Value Added Services	**Discount %** 15%

Additional Value Added Services:

Maintenance Services

Onsite Hourly Rate $ 200.00
Remote Hourly Rate $ 100.00

Professional Services

- **Deployment Services** — **Onsite Hourly Rate $** 200.00; **Remote Hourly Rate $** 100.00
- **Consulting/Advisory Services** — **Onsite Hourly Rate $** 200.00; **Remote Hourly Rate $** 100.00
- **Architectural Design Services** — **Onsite Hourly Rate $** 200.00; **Remote Hourly Rate $** 100.00
- **Statement of Work Services** — **Onsite Hourly Rate $** 200.00; **Remote Hourly Rate $** 100.00

Partner Services

Onsite Hourly Rate $ _____
Remote Hourly Rate $ _____

Training Deployment Services

Onsite Hourly Rate $ 100.00
Online Hourly Rate $ 50.00

Cost Summary

Knowledge Services has completed and provided above the Attachment G – Cost Proposal sheet for our Software as a Service (SaaS) Solution. The Discount proposed will remain fixed for the life of the contract. In our Cost Proposal Summary we have provided the pricing model and schedule for our Cloud Solution services. Our pricing model is presented at a high level utilizing Figure 1. Following the Figure, we have outlined further detail on our Cloud Solution and supporting documentation to describe our pricing model and catalog.

Throughout our 20+ years' experience providing technology and service solutions to meet government agency needs, we have developed and continuously enhanced our dotStaff™ SaaS Solution platform in order to address the increasingly complex needs of State governments. Cost savings, operational efficiencies, governance, accountability, transparency and reporting analytics are all cornerstone benefits of our Cloud Solution. Our SaaS Solution has evolved to serve wide ranging state and local government human capital management needs from information technology (IT) and general services to healthcare and medical labor categories, stationary to field-based mobile workers and contractors and Service Provider resources to government State Full Time Employees (FTE). As a proven solution deployed and operational in over 500 state agencies and departments and dozens of cities, municipalities and bodies of corporate politic, Knowledge Services offers a competitive and scalable pricing model that supports both contractor, vendor and service provider applications as well as State FTE user applications.

Figure 1

Knowledge Services (dotStaff™) Cloud Solution Options

PROVIDER
(VENDOR, SERVICE PROVIDER, SUBCONTRACTOR)

PRO SOLUTION

- CONTRACTS COMPLIANCE
- CANDIDATE PROCESS MANAGEMENT
- RESUME SUBMISSION
- RESUME SCORING
- RATING & FEEDBACK
- REVERSE AUCTION
- CANDIDATE CREDENTIALING
- INTERVIEW CALENDARING & SCHEDULING
- PRE-EMPLOYMENT COMPLIANCE
- TIME ENTRY & APPROVAL
- EXPENSE TRACKING, ENTRY & APPROVAL
- CONSOLIDATED INVOICING & PAYMENT
- FUNDING SOURCE MANAGEMENT
- REPORTING
- APPROVAL WORKFLOWS
- STATEMENT OF WORK / MILESTONE DELIVERABLE / FIXED BID FUNCTIONALITY

MOBILE PRO SOLUTION

Includes these feature from Pro Solution:

- CONTRACTS COMPLIANCE
- CANDIDATE PROCESS MANAGEMENT
- RATING & FEEDBACK
- RESOURCE CREDENTIALING
- INTEGRATED CALENDARING & SCHEDULING
- TIME ENTRY & APPROVAL
- EXPENSE TRACKING, ENTRY & APPROVAL
- CONSOLIDATED INVOICING & PAYMENT
- FUNDING SOURCE MANAGEMENT
- REPORTING
- APPROVAL WORKFLOWS
- STATEMENT OF WORK MANAGEMENT

Plus these additional features:

- ELECTRONIC DATA CAPTURE & MANAGEMENT
- LOCATION VALIDATION
- GPS TRACKING
- ROUTE OPTIMIZATION
- REAL TIME ALERTS & NOTIFICATIONS
- COLLABORATION PORTAL
- CALENDARING & SCHEDULING
- SAFETY FEATURES
- ADDITIONAL USER TYPES

FULL-TIME EMPLOYEE
FTE

PRO SOLUTION

- RATINGS & FEEDBACK
- RESOURCE CREDENTIALING
- INTEGRATED CALENDARING & SCHEDULING
- TIME ENTRY & APPROVAL
- EXPENSE TRACKING, ENTRY & APPROVAL
- CONSOLIDATED INVOICING & PAYMENT
- FUNDING SOURCE MANAGEMENT
- REPORTING
- APPROVAL WORKFLOWS
- MILESTONE MANAGEMENT

MOBILE PRO SOLUTION

Includes these feature from Pro Solution:

- RATING & FEEDBACK
- RESOURCE CREDENTIALING
- INTEGRATED CALENDARING & SCHEDULING
- TIME ENTRY & APPROVAL
- EXPENSE TRACKING, ENTRY & APPROVAL
- FUNDING SOURCE MANAGEMENT
- REPORTING
- APPROVAL WORKFLOWS
- MILESTONE MANAGEMENT

Plus these additional features:

- ELECTRONIC DATA CAPTURE & MANAGEMENT
- LOCATION VALIDATION
- GPS TRACKING
- ROUTE OPTIMIZATION
- REAL TIME ALERTS & NOTIFICATIONS
- COLLABORATION PORTAL
- SAFETY FEATURES
- ADDITIONAL USER TYPES

SERVICE PROVIDER

- PROVIDER MANAGEMENT & SUPPORT
- TRAINING
- IMPLEMENTATION
- DEDICATED PROGRAM TEAM
- SUPPORT
- CONFIGURATION
- COMPLIANCE & RISK MITIGATION
- BUSINESS ANALYTICS
- INDEPENDENT CONTRACT / 1099 VALIDATION
- RATE RATIONALIZATION & ANALYTICS
- JOB TITLE VALIDATION
- HARDWARE DEPLOYMENT
- MOBILE DEVICE MANAGEMENT
- RESUME & PHONE SCREENING
- INTERVIEW LOGISTICS COORDINATION
- BEST AND FINAL OFFER (BAFO)

Provider Pro Solution

The Knowledge Services Provider Pro Cloud Solution is designed to support the needs of State government agencies that contract with 3rd party entities for the delivery of services. The Provider Pro includes all of our Vendor Management System (VMS) Cloud Solution functionality, in conjunction with, where applicable, our Managed Service Program (MSP). The Provider Pro Solution delivers government entities robust functionality to efficiently and effectively contract temporary and contingent-based labor, utilizing existing vendors, as desired, while enabling the entire engagement processes, from procurement and time reporting to consolidated invoicing and payments, to be streamlined and automated through our SaaS Solution platform. Provider Pro is designed to deliver maximum value for government entities that contract for non-mobile, hourly labor or Statement of Work (SOW), milestone, Independent Contractor (IC/ 1099) or fixed-bid based project deliverables utilizing vendors and contractors.

Provider Mobile Pro Solution

Similar to our Provider Pro Solution, the Knowledge Services Provider Mobile Pro Cloud Solution incorporates all of the Provider Pro Vendor Management System features and capabilities, and includes powerful governance features designed to automate historically manual processes, provide accountability and support the needs of contracted mobile workers, including service provider resources. The price list we have supplied below in Figure 2 relates to our Provider Mobile Pro Workforce Solution, which includes expanded features that meet the unique needs of government agencies with contracted, vendor and / or service provider engaged field workers. Our Mobile Pro Workforce Solution SaaS platform provides for efficient management of the entire case, event and appointment-driven workforce. Provider Mobile Pro delivers complete lifecycle process automation beginning with intake and case assignment and extending to include licensing and credentialing management; calendaring and appointment scheduling management; route optimization and mileage authentication; GPS-based service and visit verification with integrated billing; real-time electronic forms and records; instant safety alerts, notifications and broadcast communications; performance ratings; time, event and activity tracking and case progress reporting, as well as predictive analytics.

Provider Mobile Pro also includes powerful tools to assist with and provide for improved communications, scheduling and experiences. These tools provide for improved outcomes:

- Vendor / provider and worker on-line ratings
- Real-time notifications of event changes including delays, cancellations and rescheduling requirements
- On-line access to documents and forms
- On-line event calendar and scheduling and change request with integrated communications to co-workers

Our Provider Pro and Provider Mobile Pro flexible pricing model offers States and agencies industry standard "vendor funded" percentage based payment method or a State funded model. In Figure 2 below, we have provided our price list for the Provider Pro and Provider Mobile Pro Solution. The percentage list price is the fee charged to the vendor / provider or Purchasing Entity by Knowledge Services based on the amount that is invoiced by Knowledge Services for work performed during a given time frame.

State FTE Pro Solution

The Cloud Solution price list supplied in Figures 1 and 3 relates to our State Full Time Employee (FTE) Workforce Management SaaS Solution, dotStaff™, in conjunction with, where applicable, our Managed Service Provider (MSP) program. The State FTE Pro Solution provides government entities and using managers a proven cloud solution that automates and streamlines State FTE worker and administrator processes, enhances communications, data access and operational reporting and provides powerful reporting analytics. With access to real-time project and State FTE worker data, State FTE Pro delivers State, agency and program leadership with unparalleled oversight and cost savings.

State FTE Mobile Pro Solution

The Cloud Solution price list supplied in Figures 1 and 4 outlines our State FTE Mobile Pro Mobile Case Management Solution, dotStaff™, which is provided in conjunction with, where applicable our MSP program services. Our State FTE Mobile Pro Solution includes all State FTE Pro Solution functionality listed above, while also delivering powerful mobile workforce management tools to help improve the safety, efficiency and effectiveness of mobile workers, as well as providing enhanced accountability, transparency and reporting. State FTE Mobile Pro delivers complete life-cycle process automation beginning with intake and case assignments; calendar and appointment scheduling management; route optimization and mileage authentication; GPS-based service verification; real-time electronic forms and records; instant safety alerts, notifications and broadcast communications; performance ratings; time, event and activity tracking and case progress reporting, as well as predictive analytics.

Our State FTE Pro and State FTE Mobile Pro flexible pricing model offers States and agencies scalable, event / activity-based pricing. In Figures 3 below, we have provided our price list for the State FTE Pro Solution. In Figure 4 below, we have provided our price list for the State FTE Mobile Pro Solution. The list price is tiered based on total State (Provider and State FTE) events. Provider and State FTE combined event volume dramatically reduces State FTE usage costs.

Price Catalog

Figure 2

State Provider Cloud Solution	List Price
Pro Solution	2.60%
Mobile Pro Solution	3.80%

Figure 3

State Full Time Employee Cloud Solution		
Pro Solution		
Total State Events	Event List Price	Event Price after 12.5% Discount
0 – 129,600	$ 4.50	$ 3.94
129,601 – 432,000	$ 4.25	$ 3.72
432,001 – 864,000	$ 4.02	$ 3.52
864,001 – 2,160,000	$ 3.86	$ 3.38
2,160,001 – 4,320,000	$ 3.73	$ 3.26
4,320,001 – 8,640,000	$ 3.64	$ 3.19
8,640,001 – 12,960,000	$ 3.57	$ 3.12
12,960,001 – 17,280,000	$ 3.54	$ 3.10
17,280,001 +	$ 3.53	$ 3.09

Figure 4

State Full Time Employee Cloud Solution		
Mobile Pro Solution		
Total State Events	Event List Price	Event Price after 12.5% Discount
0 – 129,600	$ 6.00	$ 5.25
129,601 – 432,000	$ 5.66	$ 4.95
432,001 – 864,000	$ 5.36	$ 4.69
864,001 – 2,160,000	$ 5.15	$ 4.51
2,160,001 – 4,320,000	$ 4.97	$ 4.35
4,320,001 – 8,640,000	$ 4.85	$ 4.24
8,640,001 – 12,960,000	$ 4.76	$ 4.17
12,960,001 – 17,280,000	$ 4.72	$ 4.13
17,280,001 +	$ 4.70	$ 4.11

knowledge services

Technical Proposal:
Cloud Solutions

Utah Solicitation No. CH16012
In conjunction with NASPO ValuePoint

Opening Date and Time:

Thursday, March 10, 2016, 1:00 p.m. MTN

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

knowledge services

TABLE OF CONTENTS

I. RFP Signature Page

The Lead State's Request for Proposal Signature Page completed and signed. See Section 5.1 of RFP.

Knowledge Services has provided the requested Lead State's Proposal Signature Page, completed and signed, on the following page.

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
GuideSoft, Inc. d/b/a Knowledge Services	35-1934449	

Ordering Address	City	State	Zip Code
5875 Castle Creek Parkway N Drive, Suite 400	Indianapolis	IN	46250
Remittance Address (if different from ordering address)	**City**	**State**	**Zip Code**
Same as above			

Type ☒ Proprietorship ☐ Partnership ☐ Government ☐ For-Profit Corporation ☐ Non-Profit Corporation	Company Contact Person Cindy Davis
Telephone Number (include area code) (317) 578-1700	Fax Number (include area code) (317) 578-7600
Company's Internet Web Address www.knowledgeservices.com	Email Address CindyD@knowledgeservices.com
Offeror's Authorized Representative's Signature	
Type or Print Name Julianna Bielawski	
Position or Title of Authorized Representative CEO	
Date: 3/10/2016	

12/15/2014

II. Executive Summary

The no more than three (3) page executive summary is to briefly describe the Offeror's Proposal. This summary should highlight the major features of the Proposal. It must indicate any requirements that cannot be met by the Offeror. The Lead State should be able to determine the essence of the Proposal by reading the executive summary. See Section 5.4 of the RFP.

Knowledge Services is pleased to present our proposal to the State of Utah, in conjunction with NASPO ValuePoint. Knowledge Services' Cloud Solution, dotStaff™, is a Vendor Management System (VMS) and Mobile Workforce Solution, providing government entities a web-based, mobile-accessible platform that allows organizations to easily engage and govern their entire workforce management programs, including contingent workers, contractors and Independent Contractors (IC / 1099s), service providers and State full time employees (FTEs). The dotStaff™ Software as a Services (SaaS) platform incorporates the entire workforce engagement and oversight process, including sourcing management, assignment management, communication management, time and activity tracking, progress reporting and billing, as well as secure document sharing and a vehicle for advanced predictive analytics, in a user-friendly, configurable application that increases efficiency, provides improved governance and accountability, reduces costs and drives compliance throughout an organization.

Knowledge Services, utilizing its cloud-based dotStaff™ technology, currently holds prime contracts in seven State governments, including hundreds of State agencies and several dozen cities and municipalities across the United States. Using Knowledge Services' dotStaff™ SaaS Cloud Solution, our government clients have driven measurable improvements throughout their workforce management programs. Our comprehensive application is highly scalable and flexible so as to meet the needs of complex government organizations. Our government clients utilize our Cloud Solution for all skill and labor categories, including medical and health sciences, information technology, accounting and finance, administrative and clerical, engineering, professional, call center and all general services.

The Knowledge Services dotStaff™ Solution is the only provider in State government that supports all traditional and non-traditional contingent and temporary labor categories. dotStaff™ is also the only State government-deployed SaaS platform for the procurement, mobile management and workforce management process that supports stationary State Full Time Employees (FTEs), State mobile FTEs, mobile contract workers, contracted vendor and service provider workers who travel from site to site or from appointment to appointment.

In serving government needs for vendor management, dotStaff™ addresses requirements for managing vendor-based contingent and temporary labor, fixed-bid and milestone Statement of Work (SOW) and field-based mobile and in-home service provider management. Utilizing the dotStaff™ SaaS platform, government entities are able to improve operational efficiencies, provide improved governance and accountability and improve information access for field and mobile based workers.

Knowledge Services' Cloud Solution meets the requirements of the RFP.

The major features of the Knowledge Services Cloud Solution are:

- Contracts Compliance
- Candidate Process Management
- Resume Submission
- Resume Scoring
- Rating & Feedback
- Reverse Auction
- Candidate Credentialing
- Calendaring & Scheduling
- Pre-Employment Compliance
- Time Entry & Approval
- Expense Tracking, Entry & Approval
- Consolidated Invoicing & Payment
- Funding Source Management
- Reporting & Business Analytics
- Approval Workflows
- Statement of Work / Milestone Deliverable / Fixed-Bid Functionality
- Electronic Data Capture & Management
- Location Validation
- GPS Tracking
- Route Optimization
- Real-Time Alerts & Notifications
- Collaboration Portal
- Safety Features
- Additional User Types

The Solution's growth, overall use and acceptance has been driven by its unique and broad functionality, supported by superior, customer service oriented MSP Program services. dotStaff™ is highly configurable and, therefore, can be configured to meet and adapt to the evolving governmental demands. As governments continue to look for savings opportunities, and are constantly challenged to do more with less, validating activity around their entire workforce within a single, cloud-based platform has proven to provide significant value.

There are two major Solutions within our SaaS technology: 1) Pro Solution and 2) Mobile Pro Solution. The Knowledge Services dotStaff™ Pro Solution provides government entities a Vendor and Contract Management System, supported by our Managed Service Provider (MSP) Program, that focuses on improving and facilitating the hiring process for their contingent and State FTE labor needs. Our clients benefit from one point of contact who manages, on their behalf, the entire contingent labor process from requisition and contract management to billing and invoicing to reporting and business analytics. Our Pro Solution provides State governments with hard dollar cost savings through reverse auction and rate card management; improved compliance and risk mitigation through streamlined vendor / contractor credentialing and Independent Contractor / 1099 compliance; and automated processes and approval workflows to simplify the entire contingent and State FTE workforce process.

The Knowledge Services dotStaff™ Mobile Pro Solution provides a total cost of ownership (TCO) on a single integrated platform. Our clients benefit from streamlined access to critical business intelligence (BI) allowing for informed decision making with real-time, accurate data and analytics that improve citizen outcomes and internal processes. The Mobile Pro Solution provides essential fraud prevention capabilities as well as time, date, location and duration validation activities for the entire workforce – stationary, mobile, State FTE and contractor. Our SaaS Solution provides route optimization with an integrated calendaring and scheduling component that offers real-time alerts and notifications, including an embedded "Panic" button allowing field personnel to document safety concerns and covertly send for assistance. The Mobile Pro Solution provides both leadership and field staff with time saving process efficiencies to improve outcomes and quality of service.

III. Mandatory Minimums (Section 5)

This section should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.

Knowledge Services is pleased to present our proposal to the State of Utah, in conjunction with NASPO ValuePoint. This section includes our point-by-point response to each of the items described in Section 5 of the RFP, except Section 5.1 (which is included above beginning on page 4) and Section 5.4 (which is included above beginning on page 6).

Cover Letter (Section 5.2)

Proposals must include a cover letter on official letterhead of the Offeror. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed. In addition, the cover letter must include:

- *5.2.1 A statement indicating the Offeror's understanding that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.*
- *5.2.2 A statement naming the firms and/or staff responsible for writing the proposal.*
- *5.2.3 A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.*
- *5.2.4 A statement acknowledging that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.*
- *5.2.5 A statement identifying the service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) that it is capable of providing under the terms of the RFP. See Attachment C for a determination of each service model subcategory. The services models, deployment models and risk categories can be found in the Scope of Services, Attachment D. Note: Multiple service and/or deployment model selection is permitted, and at least one service model must be identified. See Attachment H.*
- *5.2.6 A statement identifying the data risk categories that the Offeror is capable of storing and securing. See Attachment D and Attachment H.*

Knowledge Services has provided the requested cover letter addressing each item from Sections 5.2.1 – 5.2.6 on official letterhead on the following page.

knowledge services

March 10, 2016

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

Dear Mr. Hughes,
Knowledge Service is pleased to present our proposal for Cloud Solutions – Utah Solicitation Number CH16012 for the State of Utah, in conjunction with NASPO ValuePoint Cooperative Purchasing Program. Established in 1994 and headquartered in Indianapolis, Indiana, GuideSoft Inc. d/b/a Knowledge Services is a certified Woman-Owned Business Enterprise (WBE) professional services corporation.

Knowledge Services' Cloud Solution will provide the State a proven solution to procure, manage, report and analyze staff augmentation and the mobile workforce. Our Cloud Solution is a proven and repeatable model, providing State governments with predictable, low risk and meaningful results.

The Knowledge Services team members understand and agree that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

The response to this RFP was prepared by the following individuals:

- Joe Bielawski, President
- Dave Stenger, Vice President, dotStaff™ Solution
- Damon Grothe, Vice President
- Cindy Davis, Director
- Emily Kirchmann, Research Associate

Knowledge Services is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

Knowledge Services understands and acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from this RFP.

The service and deployment model that Knowledge Services is capable of providing under the terms of the RFP is Software as a Service (SaaS) and the deployment model is Private Cloud. Our Cloud Solution is capable of storing and securing low and moderate risk data.

On behalf of the entire Knowledge Services team, we appreciate and look forward to the opportunity to work with the State of Utah and NASPO ValuePoint.

Sincerely,

CEO

Julianna Bielawski
CEO
Knowledge Services

KnowledgeServices
Toll Free: 877.256.6948
Office: 317.578.1700
Fax: 317.578.7600
5875 Castle Creek Parkway, Suite 400
Indianapolis, IN 46250
www.KnowledgeServices.com

Acknowledgement of Amendments (Section 5.3)

If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive.

Knowledge Services acknowledges the RFP was amended; please find below an executed Acknowledgement of Amendments signature form.

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.

Guidesoft, Inc., dba Knowledge Services
Offeror

Representative Signature

General Requirements (Section 5.5)

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

Knowledge Services understands and agrees that, if awarded a contract, we will provide a Usage Report Administrator responsible for the quarterly sales reporting as described in the Master Agreement Terms and Conditions, as well as any additional report requirements established with 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.

Knowledge Services understands and agrees to cooperate with NASPO ValuePoint and SciQuest (as well as any authorized agent or successor entity to SciQuest) with uploading our ordering instructions, if awarded a contract.

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

Knowledge Services meets the requirement to provide a completed CSA STAR Registry Self-Assessment and has completed and provided as separate attachments The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B and compliance with Cloud Controls Matrix (CCM), Exhibit to Attachment B. The information provided in the attachment is complete and accurate.

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.

Knowledge Services understands the importance of meeting and exceeding Service Level Agreement (SLA) requirements. We constantly measure, monitor and review SLA's to ensure compliance. We have provided below our sample SLA, which defines the performance and other operating parameters.

Service Level Agreement ("SLA")

This document outlines the service levels to be provided in the delivery of SaaS. It also provides service delivery parameters, against which the delivery of SaaS will be evaluated. The SLA provides certain rights and remedies in the event that the Customer experiences service interruption as a result of failure of dotStaff™ infrastructure.

Service uptime commitment

THIS SERVICE LEVEL AGREEMENT ("Agreement" or "SLA") shall apply to all Services provided by dotStaff™ expressly as an addendum to the Terms of Service ("TOS") for each customer / client / vendor / end user ("USER"). dotStaff™ is committed to providing a highly available and secure service to support its USERs. Providing the USER with consistent access to dotStaff™ Services is a high priority for dotStaff™ and is the basis for its commitment in the form of a SLA. The SLA provides certain rights and remedies in the event that the USER experiences service interruption as a result of failure of dotStaff™ infrastructure. The overall service availability metric is 99.9%, measured on a monthly basis.

This Service Level Agreement shall only become applicable to dotStaff™ Services upon the later of (a) completion of the "implementation period," as such term is defined in the Statement of Work (if any), or (b) ninety (90) days from contract effective date.

1. Term Definitions

Available or Availability
When the USER who's account is active and enabled has reasonable access to services provided by dotStaff™, subject to the exclusions defined in Downtime Minutes below.

Total Monthly Minutes
The number of days in the month multiplied by 1,440 minutes per day.

Maintenance Time
The time period during which dotStaff™ Service may not be available each month so that dotStaff™ can perform routine maintenance to maximize performance, is on an as needed basis.

Downtime
The total number of minutes that the USER cannot access the dotStaff™ Service. The calculation of Downtime Minutes excludes time that the USER is unable to access dotStaff™ Services due to any of the following:

i. Maintenance Time
ii. USER's own Internet service provider
iii. Force Majeure event
iv. Any systemic Internet failures
v. Enhanced Services
vi. Any failure in the USER's own hardware, software or Network connection
vii. USER's bandwidth restrictions
viii. USER's acts or omissions
ix. Anything outside of the direct control of dotStaff™

2. dotStaff Maintenance

Maintenance Notices
dotStaff™ will communicate the date and time that dotStaff™ intends to make dotStaff™ Services un-Available via the front page of the dotStaff™ product web site at least forty-eight (48) hours in advance (or longer if practical). The USER understands and agrees that there may be instances where dotStaff™ needs to interrupt dotStaff™ Services without notice in order to protect the integrity of dotStaff™ Services due to security issues, virus attacks, spam issues or other unforeseen circumstances. Below are the Maintenance Windows and their definitions:

Emergency Maintenance
These change controls happen immediately with little notification ahead of time.

Preventative Maintenance
These change controls are when we detect an item in the environment that we need to take action on, to avoid emergency change controls in the future. These change controls, if possible, will usually occur during our planned maintenance window. If this is not possible, they will occur in low peak hours with peak being defined by our network metrics.

Planned Maintenance
These are change control's being done to:

Support on-going product and operational projects to ensure optimal performance
Deploy non-critical service packs or patches.
Periodic redundancy testing.

Where possible planned maintenance will be posted 5-days prior; however, certain circumstances may preclude us from doing so. Planned maintenance windows are Saturday mornings between 8:00am and 12:00pm EST.

3. Measurement

dotStaff™ uses a proprietary system to measure whether dotStaff™ Services are Available and the USER agree that this system will be the sole basis for resolution of any dispute that may arise between the USER and dotStaff™ regarding this Service Level Agreement.

Availability is calculated based on the following formula:
A = (T – M – D) / (T – M) x 100%
A = Availability
T = Total Monthly Minutes
M = Maintenance Time
D = Downtime

4. Software-as-a-Service Credits

Financial Consequences for Non-Performance
Measured Enterprise-wide per month based on minimum performance target (not occurrence)
Maximum credit amount is $500 per month per contract.

Quarterly SaaS rating	Rating	SaaS service credit
Between 99.9% - 100%	Meets Goal	
Between 99.0% - 99.8%	Tolerable	$150 / month
Below 99.0%	Unacceptable	$500 / month

5. User Responsibility

Minimum Requirements
The required configurations USER must have to access dotStaff™ Services include:

Internet connection with adequate bandwidth
Supported Internet Browser

Remedy and Procedure
The USER's remedy and the procedure for obtaining the USER's remedy in the event that dotStaff™ fails to meet the Service level metrics set forth above are as follows:

To qualify for remedy
(a) There must be a support ticket documenting the event within 24 hours of the service interruption
(b) USER account must be in good standing with all invoices paid and up to date

The USER must notify dotStaff™ in writing within five (5) business days by opening a support ticket and providing the following details:

Subject of email must be: "Claim Notice – dotStaff™ Service Downtime"
List the type of Service that was affected
List the date the Downtime Minutes occurred
List user(s) Login Name and E-mail address affected by Downtime Minutes
List an estimate of the amount of actual Downtime Minutes
Ticket number of the documented event

dotStaff™ will confirm the information provided in the Claim Notice within ten (10) business days of receipt of the Claim Notice. If dotStaff™ cannot confirm the Downtime Minutes, then the USER and dotStaff™ agree to refer the matter to executives at each party for resolution. If dotStaff™ confirms that dotStaff™ is out of compliance with this Service Level Agreement, the USER will receive the amount of Service Level Credits set forth above for the affected Service level metric for the affected month. The SLA credit will be reflected in the dotStaff™ invoice to the USER in the invoice cycle following dotStaff™ confirmation of the Downtime Minutes. Please note that SLA credits can only be applied to accounts that are in good standing with all invoices paid and up to date.

Recertification of Mandatory Minimums and Technical Specifications (Section 5.7)

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

Knowledge Services acknowledges and will comply with the requirement to annually certify to the Lead State that our Cloud Solution still meets and / or exceeds the technical capabilities discussed in the proposal.

IV. Business Profile

This section should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 6 of the RFP.

Knowledge Services has read Section 6 of the RFP. Below is Knowledge Services' specific point-by-point response, in the order listed, to each requirement.

Business Profile (Section 6.1)

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

Knowledge Services, founded in 1994 by our CEO, Julie Bielawski, has been a leading provider of cloud-based Vendor Management System (VMS) and Mobile Workforce Solutions for over 12 years. Utilizing our dotStaff™ Cloud Solution in combination with our Managed Service Provider (MSP) program services, we've established an industry-acknowledged expertise, serving the needs of State and City governments and Fortune 500 clients alike. Knowledge Services is a privately held certified Woman-Owned Business Enterprise (WBE) corporation with approximately 1,500 employees located in offices throughout North America.

Our organizational structure includes a centrally-based leadership team comprised of the following individuals, and supported by regionally-based client managers and industry experienced support teams:

- Julie Bielawski, CEO
- Joe Bielawski, President
- Bill Evans, Vice President, Programs
- Damon Grothe, Vice President, Professional Services
- Dave Stenger, Vice President, Product Development
- Brian Fiscus, Chief Financial Officer
- Katie Belange, Corporate Counsel

We are experts in and primarily focus on delivering, supporting and administering the dotStaff™ cloud Solution to our clients for their comprehensive Vendor Management System (VMS), Managed Service Provider (MSP), mobile case management and related mobile workforce needs, and specifically serving State and local governments. With proven experience in implementing, managing and operating VMS, MSP, mobile case management and mobile workforce Solutions, Knowledge Services addresses the specific and current challenges faced by State governments. Knowledge Services delivers unsurpassed service quality, cost savings, transparency and governance to seven State governments, including over 500 State agencies and departments each with unique workflows and agency-level requirements, multiple city governments, counties and municipalities, political bodies, universities and other cooperatives. Knowledge Services has become a recognized industry leader and expert at providing VMS, MSP, mobile case

management and mobile workforce Solutions for contingent, State Full-Time Employee (FTE) and the mobile worker to the government market vertical.

Our client base focus is State government and includes over 500 State agency and department clients representing Federal, State and local governments, including universities and quasi-governmental entities, and commercial corporations from the medical and health services, financial and insurance, manufacturing and distribution, retail and food services, entertainment, and technology industries. Our dotStaff™ Cloud Solution is accessible and utilized globally.

Our Government Solutions team is dedicated to the effective and efficient management of our program services including reducing risks, providing increased governance, accountability and controls, enhancing workforce decision support and delivering cost savings for governments and agencies. Our cloud-based projects range from dozens of users to thousands, both stationary and mobile workers and physical locations ranging from a single site to hundreds of locations throughout the United States.

With an employee retention rate exceeding 98%, our Government Solutions team has the experience and depth to implement and manage our cloud-based Solution for State government. The Government Solutions leadership team is comprised of seven team members who may be directly engaged in services related to our proposed Cloud Solution:

- Joe Bielawski – Employee since 1994
- Bill Evans – Employee since 2009
- Damon Grothe – Employee since 2013
- Dave Stenger – Employee since 2004
- Cindy Davis – Employee since 2005
- Andrea Connell – Employee since 2009
- Brett Nagel – Employee since 2005

Our experience and growth in recent years as the prime contractor for our cloud-based Solution in conjunction with our MSP Program service, includes State government contracts with the States of Indiana, Arizona, Maine, Tennessee, Florida, Utah and Ohio. Our extensive, large scale (serving hundreds of organizationally complex State agencies), Cloud Solution experience with State and local governments span seven years of continuous service.

Meeting the required minimum of three years of experience providing Cloud Solutions for large scale projects, including government experience, is our experience with the States of Indiana, Arizona and Maine. In the Scope of Experience section below, we have provided our experience and scope providing Cloud Solutions to the States of Indiana, Arizona and Maine, as well as States of Tennessee and Florida.

Scope of Experience (Section 6.2)

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

Knowledge Services has business experience with government contracts similar to the Master Agreements sought through this RFP with the States of Indiana, Arizona, Maine, Tennessee and Florida. With numerous State government Vendor Management System (VMS) / Managed Service Provider (MSP) Program prime contractor engagements and dozens of municipality engagements, years of proven experience, thorough documentation, detailed process driven methodologies, financial strength and an unparalleled breadth of skills served (IT, clerical / administrative, medical, etc.), Knowledge Services has the capacity and is especially qualified to meet the needs of the State of Utah and other Purchasing Entities.

Below we have provided our business' experience with government contracts similar in scope providing Cloud Solutions to the States of Indiana, Arizona, Maine, Tennessee and Florida.

Experience 1:

Client Name:	State of Indiana
Solutions Provided:	dotStaff™ VMS Cloud Solution, in conjunction with MSP Program
Contingent Labor Categories Managed:	Information technology, professional services, Statement of Work (SOW) projects, clerical / administrative and medical positions, all other general services categories
Years as a Client:	7 years. Implemented in February 2009 – Current.
Current Approximate Dollar Value:	$372 million
Program Size / Volume	
Number of IT Positions Filled for CY 2015:	246
Number of Concurrently Engaged IT Resources:	251
Most Recent Full Year Spend:	$62 million
Hard Dollar Savings:	$46 million
Client Contact Information	
Contact Name:	Mark Hempel
Contact Title:	Senior Account Manager
Department:	Indiana Department of Administration
Address:	402 W Washington Street, Room W468, Indianapolis, Indiana 46204
Telephone:	(317) 232-2498
Email Address:	mhempel@idoa.in.gov

Implemented February 2009, with the goals of enhancing resource quality, improving resource retention, reducing costs, increasing Indiana Economic Impact and gaining greater command and control through a centralized database and reporting system, the State of Indiana sought to procure a MSP with VMS Solution for contingent IT labor. Following an extensive RFI, RFP and multiple oral presentations to a committee of 16 individuals, the State of Indiana selected Knowledge Services from a group of nine national MSP and VMS finalists. Prior to RFP and Award, the State of Indiana Office of Technology (IOT) utilized a "preferred vendor" arrangement with 18 vendors. During the discovery phase of implementation, Knowledge Services learned there were actually over 60 vendors billing through multiple higher-level sub-vendors. Within two years, based on the Knowledge Services MSP Program exceeding the State's expectations, Knowledge Services was asked to expand its services to include Statement of Work (SOW) projects, medical, seasonal workers and administrative, and finance and accounting contingent labor within all State of Indiana Agencies. The Knowledge Services VMS / MSP Program also includes a variety of Cooperatives such as Quasi-Agencies, Cities / Municipalities, and Universities. Knowledge Services has saved the State of Indiana over $45 million in hard dollar cost savings since go live through the use of the dotStaff™ Cloud Solution and MSP Program services.

Experience 2:

Client Name:	State of Arizona
Solutions Provided:	dotStaff™ VMS Cloud Solution, in conjunction with MSP Program
Contingent Labor Categories Managed:	Information technology and Statement of Work (SOW) project work
Years as a Client:	3.5 years. Implemented in October 2012 – Current.
Current Approximate Dollar Value:	$188 million
Program Size / Volume	
Number of Positions Filled for CY 2015:	492
Number of Users:	1721
Number of Concurrently Engaged Resources:	577
Most Recent Full Year Spend:	$70 million
State of Arizona Cooperatives Usage:	15 Cooperatives utilize Solution
Hard Dollar Savings:	$16 million
Client Contact Information	
Contact Name:	Terri Johnson
Contact Title:	Procurement Manager (Strategic)
Department:	State Procurement Office
Address:	ADOA Building, 100 N. 15th Avenue, Suite 201, Phoenix, Arizona 85007
Telephone:	(602) 542-9122 or (602) 267-2853
Email Address:	Terri.johnson@fmo.azdema.gov or terri.johnson@azdoa.gov

Implemented in October 2012, with key goals of adding value, reducing costs and increasing productivity by offloading administrative duties and improving operations, the State of Arizona sought to procure a VMS / MSP Program for the contingent IT labor. As a result of the State's RFP release, Knowledge Services was selected to implement and manage the State's Information Technology Professional Services Contract as the awarded VMS / MSP Program. The Knowledge Services VMS / MSP Program also includes a variety of Cooperatives such as Quasi-Agencies, Cities / Municipalities and Universities. Knowledge Services has saved the State of Arizona over $16 million in hard dollar savings since inception through the use of the dotStaff™ Cloud Solution and MSP Program services.

Experience 3:

Client Name:	State of Maine
Solutions Provided:	dotStaff™ VMS Cloud Solution, in conjunction with MSP Program
Contingent Labor Categories Managed:	Information technology
Years as a Client:	3.5 years. Implemented in December 2012 – Current.
Current Approximate Dollar Value:	$55 million
Program Size / Volume	
Number of Positions Filled:	213
Number of Users:	601
Number of Concurrently Engaged Resources:	180
Most Recent Full Year Spend:	$19 million
State of Maine Cooperatives Usage:	1 Cooperative utilizes our Solution
Client Contact Information	
Contact Name:	Michelle Fournier
Contact Title:	Director of Special Projects
Department:	Office of Information Technology
Address:	145 State House Station, Augusta, Maine 04333
Telephone:	(207) 624-8868
Email Address:	Michelle.Fournier@maine.gov

Implemented in December 2012, with key goals of adding value, enhancing resource quality and retention, increasing local vendor utilization and increasing productivity by offloading administrative duties and improving operations, the State of Maine conducted a procurement to source a VMS / MSP Program Solution for contingent IT labor. As a result of the State's RFP release, Knowledge Services was selected to implement and manage the State's IT contingent labor contract as the awarded VMS / MSP. Knowledge Services replaced another MSP provider and dotStaff™ replaced another VMS Cloud Solution at the State of Maine.

Experience 4:

Client Name:	State of Tennessee
Solutions Provided:	dotStaff™ VMS Cloud Solution, in conjunction with MSP Program
Contingent Labor Categories Managed:	Information technology, medical and general services
Years as a Client:	2.5 years. Implemented in October 2013 – Current.
Current Approximate Dollar Value:	$68 million
Program Size / Volume	
Number of Positions Filled:	639
Avg. Headcount Entering Time (per Quarter):	747
Most Recent Full Year Spend:	$31 million
Hard Dollar Savings:	$9.3 million

Implemented October 2013, with the goals of adding value in contingent worker procurement and utilization, reducing costs, minimizing time spent engaging contingents, ensuring compliance, monitoring and managing vendor performance, reporting, providing visibility, aligning job descriptions and increasing the overall quality and speed of contingent worker procurement. Following an RFP and oral presentation, the State of Tennessee selected Knowledge Services, in conjunction with dotStaff™ VMS, from a group of eleven proposals. The State of Tennessee's RFP included information technology (IT), healthcare / medical, and general services contingent labor. Knowledge Services has saved the State of Tennessee over $9.3 million in hard dollar savings since inception, utilizing the dotStaff™ Cloud Solution and MSP Program services.

Experience 5:

Client Name:	State of Florida
Solutions Provided:	dotStaff™ VMS Cloud Solution, in conjunction with MSP Program
Contingent Labor Categories Managed:	Administrative and light industrial
Years as a Client:	1+ years. Implemented in November 2014 – Current.
Current Approximate Dollar Value:	$9 million
Program Size / Volume	
Number of Positions Filled:	544
Number of Concurrently Engaged Resources:	1,048
Most Recent Full Year Spend:	$9 million

Implemented in November 2014, with key goals of quickly and efficiently acquiring contingent administrative and light industrial staff in a vendor-neutral process and system, the State of Florida utilized the State of Indiana's competitive procurement process and cooperative language to enter into an Agreement for a VMS / MSP Program Solution with Knowledge Services.

Financials (Section 6.3)

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

As a financially strong and stable, privately-held company, Knowledge Services provides outstanding prime contractor services to major organizations and Fortune 500 companies in various industries, including Federal and State governments, public utilities / telecom, healthcare, media and entertainment, manufacturing and other sectors. Knowledge Services has a stable financial track record of consistent and profitable growth, including a strong balance sheet, which is substantiated with the attached schedules. Knowledge Services possesses the financial capability to assure good faith performance of the Contract. We are proud of our consistent and stable revenue growth over the past several years.

Year 2008	$18.5 million
Year 2009	$26.3 million
Year 2010	$57.3 million
Year 2011	$72.6 million
Year 2012	$84.8 million
Year 2013	$159.0 million
Year 2014	$214.8 million
Year 2015	$273.8 million

Please refer to the "Confidential, Protected or Proprietary Information" section of the RFP to find our financial statements and recognized rating to demonstrate we are financially responsible for performance of the agreement. As Knowledge Services is a privately-held company, we request that our financial information be held as confidential and not made available to the public.

General Information (Section 6.4)

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

Introduced to the market in 2004 as a Software as a Service (SaaS) Vendor Management System (VMS), dotStaff™ was designed to streamline the temporary and contract staffing requisition, time tracking and vendor payment management processes. The design enabled clients to procure the right resource, at the right time, for the best price. The dotStaff™ system provided clients and temporary staffing vendors with transparency, free enterprise / competitive pricing and governance. Today, the Knowledge Services dotStaff™ cloud-based SaaS Solution, being used by hundreds of State agencies, cities, municipalities and bodies of corporate politic, has been awarded and is in use by more government entities than any solution of its kind, including the State of Utah.

Since dotStaff™'s inception, Knowledge Services has focused on serving client needs for all labor categories, including information technology (IT), administrative / clerical, finance / accounting, medical, general services including all support and ancillary roles. Employing Agile development methodology, the dotStaff™ SaaS Solution has continually been enhanced to serve the ever greater needs of government. In conjunction with our Managed Service Provider (MSP) Program services, dotStaff™ is used today for both vendor management and where applicable, State full-time mobile employee process automation and oversight.

In serving government needs for Vendor Management, dotStaff™ addresses requirements for managing vendor based contingent and temporary labor, fixed-bid, milestone Statement of Work (SOW), Independent Contractor (IC / 1099) and field-based mobile and in-home service provider management. Utilizing the dotStaff™ SaaS platform government entities are able to improve operational efficiencies, provide improved governance and accountability and improve information access of field and mobile based workers.

The Solution's growth, overall use and acceptance has been driven by its unique and broad functionality, supported, where applicable, by superior, customer service oriented MSP Program services. dotStaff™ is highly configurable and, therefore, can be configured to meet and adapt to the evolving governmental demands. As governments continue to look for savings opportunities, and are constantly challenged to do more with less, validating activity around their entire workforce within a single, cloud-based platform has proven to provide significant value.

The Knowledge Services dotStaff™ Solution is the only provider in State government that supports all traditional and non-traditional contingent and temporary labor categories. dotStaff™ is also the only State government deployed SaaS platform for the procurement, mobile case management and workforce management processes that supports stationary State Full-Time Employees (FTEs), State mobile FTEs, mobile contract workers, contracted vendor, Independent Contractor (IC / 1099) and service provider workers who travel from site to site or from appointment to appointment.

The Knowledge Services dotStaff™ Pro Solution provides government entities a Vendor and Contract Management System, supported by our Managed Service Provider Program, that focuses on improving and facilitating the hiring and contracting process for their contingent and State FTE labor needs. Our clients

benefit from one point of contact who manages, on their behalf, the entire contingent labor process from requisition and contract management to billing and invoicing to reporting and business analytics. Our Pro Solution provides State governments with hard dollar cost savings through reverse auction and rate card management; improved compliance and risk mitigation through streamlined credentialing and Independent Contractor / 1099 compliance; and automated processes and approval workflows to simplify the entire contingent and State FTE workforce process.

The Knowledge Services dotStaff™ Mobile Pro Solution provides a total cost of ownership (TCO) on a single integrated platform. Our clients benefit from streamlined access to critical business intelligence (BI) allowing for informed decision making with real-time, accurate data and analytics that improve citizen outcomes and internal processes. The Mobile Pro Solution provides essential fraud prevention capabilities as well as time, date and location validation activities for the entire workforce – stationary, mobile, State FTE and contractor. Our SaaS Solution provides route optimization with an integrated calendaring and scheduling component that offers real-time alerts and notifications. All designed to provide leadership and field workers with increased efficiencies for improving outcomes and quality of service.

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.

Knowledge Services' auditing capabilities and reports are consistent with SSAE 16. SOC 1 and SOC 2 Reports are attached in the Appendix.

Billing and Pricing Practices (Section 6.5)

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

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

The Knowledge Services dotStaff™ SaaS Solution is designed with an automatic invoice generation system. Configurable billing intervals permit wide-ranging client requirements to be met and multiple levels of detail are available with the standard consolidated invoices. The invoice can provide breakouts by agency, user, projects, PO number, funding source, managers and account line, etc. The dotStaff™ Solution provides for on-line and mobile access and includes fully-auditable transaction history. dotStaff™ has the flexibility to accommodate funding source needs and is broken out by labor type, Provider Pro, Provider Mobile Pro, FTE Pro and FTE Mobile Pro.

The Provider Pro and Provider Mobile Pro Solution pricing models are based on a percentage fee of total Provider billings of approved time and milestones and can be vendor funded or State funded. The FTE Pro and FTE Mobile Pro Solution pricing models are structured on events and / or appointments that are system validated. All invoice and billing transactions, whether hourly, milestone, event and / or appointment based, are available on-line and provide unprecedented transparency, within the Solution's security profile, to all appropriate users including client administrators, client managers, vendors and service providers.

Knowledge Services supports both electronic and / or printed invoices with summary and detail data, configured to the Purchasing Entity's requirements. The dotStaff™ Cloud Solution allows an approver to define backup approvers as needed or on a case by case basis to cover situations such as vacation, illness, etc.; there is not a limit to the number of approvers.

The system is designed to allow significant flexibility, recognizing that various Purchasing Entity users may have a variety of approval requirements and / or workflows. There is flexibility in the system for user defined titles and fields which would be customized during implementation discovery sessions.

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

The Knowledge Services Provider Pro and State Full Time Employee (FTE) Pro Solutions typically require program-specific configuration. State governance, procurement, system security definitions and legacy system integrations are but a few of the considerations that must be addressed throughout system implementation and use. Following is a list of possible cost components that may influence a Purchasing Entity's cost impact decision matrix, solution justification and / or Return on Investment calculation:

- Implementation consulting
- Training
- Hardware
- Hardware accessories
- Integrations / interfaces
- Storage
- Maintenance
- Client-specific custom developed forms

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.

Knowledge Services Solution is NIST compliant. Our Cloud Solution is a Software as a Service (SaaS) model and accessible from a web browser. The Purchasing Entities do not manage or control the underlying infrastructure, such as network, servers, operating systems or storage. The essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service) are transparent to the Entities. Broad network access is achieved via a web browser, but provision of computing capabilities, resource pooling, elasticity and measured service is managed by the Offeror.

Scope and Variety of Cloud Solutions (Section 6.6)

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

This solicitation response is for a Software as a Service (SaaS) Solution for our Knowledge Services Provider Pro, Provider Mobile Pro, State Full Time Employee (FTE) Pro, State FTE Mobile Pro and Vendor Management System (VMS) Solutions. Our cloud-based Vendor Management System (VMS), in conjunction with Managed Services Provider (MSP) program services, and Mobile Workforce Solutions are designed and have been proven in hundreds of State agencies to meet government needs relating to procurement and management of vendor and service provider based labor as well as State FTEs, both stationary and mobile workers.

Our dotStaff™ Solution platform, in conjunction, where applicable, with our MSP programs, serve the needs of State governments whose objectives are for reduced costs, improved governance, vendor management and consolidated billings, accountability, service verification, savings and transparency relating to labor driven activities. Whether contracted, temporary, service-based, milestone deliverable, patient-centered, case-based or State FTEs, the dotStaff™ Solution provides unparalleled process automation and operational efficiencies.

Supporting all labor categories including information technology (IT), health and medical, administrative and general services, professional, etc. the dotStaff™ Solution supports all labor types and program scope of use. Traditional "in–house" labor category uses of IT, medical and administrative are easily served with our SaaS Solution. Additional value comes from savings, resource accountability, field worker and citizen safety, governance, service verification and predictive analytics resulting from mobile worker categories including in-home health services, case workers, auditors, investigators and others.

All labor activities, whether contracted or State FTE, are easily identified, tracked, verified and reported on from within the Knowledge Services dotStaff™ SaaS platform. Specific Solution functionalities may vary based on agency by agency application needs and can be configured accordingly, all from the same SaaS platform.

Best Practices (Section 6.7)

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

Knowledge Services policies and procedures meet the requirement to restrict visibility of cloud-delivered data and documents to specific users and / or groups. With multiple State governments, the dotStaff™ Solution was designed with configuration controls which can be conformed to each State agency's needs, at no additional cost to the State. The dotStaff™ Solution is configurable to support multiple State user groups as well as multiple user roles according to access to necessary data and functionality.

The dotStaff™ Solution meets this requirement through its role-based security model. Roles include: dotStaff™ Administrator, Client Administrator, Client User, Vendor Administrator, Vendor User, Resource and

MSP, with the ability to include additional user roles such as patient, caregiver and guardian. The configuration options in the dotStaff™ VMS allow one to assign "view" and "edit" access to a specified subset or group of roles, enabling rights to perform various functions as needed. All users must be authenticated before gaining access to the dotStaff™ Solution. Once authenticated by username and encrypted password, specific application roles are used to grant access to specific data by specific role types. Form and field-based security can also be identified in specified user areas within the dotStaff™ Solution.

Our SaaS Solution policies and procedures provide compliance to our clients through our risk mitigation during the implementation process. Knowledge Services will meet with the Purchasing Entity, cooperate and hold a meeting(s) to determine whether any sensitive or personal information will be stored or used that is subject to any law, rule or regulation providing for specific compliance obligations. As standard practice with each new Program, our deployment team completes an initial findings meeting and subsequently, as needed, a discovery phase. The purpose of the findings meeting and discovery phase is to determine the configuration requirements and types of data to be stored. A report of findings and subsequent sign-off by the procuring entity, ensures that both parties are aware and agree to any security steps required to meet compliance obligations.

The dotStaff™ Solution encrypts data in transit via a 2048bit SSL certificate over HTTPs. Data elements that require encryption at rest are encrypted using an MD5 cryptographic hash.

V. Organization Profile

This section should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 7 of the RFP.

Knowledge Services has read Section 7 of the RFP. Below is Knowledge Services' specific point-by-point response, in the order listed, to each requirement in this section.

Contract Manager (Section 7.1)

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

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.

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.

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.

Knowledge Services will meet and exceed the requirement to 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 Knowledge Services Contract Manager is Cindy Davis.

Contract Manager Name: Cindy Davis
Phone Number: (317) 806-6104
Email Address: CindyD@knowledgeservices.com
Work Hours: Monday – Friday from 8:00 AM – 5:00 PM EST

Cindy has experience managing contracts for our Knowledge Services Cloud Solutions for multiple State contracts including, but not limited, to the States of Florida, Utah and Ohio. These State contracts are similar in size and scope to the one that will be awarded from this RFP.

	Contract 1	Contract 2	Contract 3	Contract 4	Contract 5
Entity Type	State Government	State Government	State Government	State Government	State Government
State the Entity is Located	Indiana	Arizona	Maine	Tennessee	Florida
Scope of Project	VMS / MSP Program for all labor categories including IT, IT SOW projects, admin / clerical and	VMS / MSP Program for IT and IT SOW projects	VMS / MSP Program for IT and IT SOW projects	VMS / MSP Program for all labor categories including IT, IT SOW projects, admin / clerical and	VMS / MSP Program for administrative and light industrial

	medical			medical	
Size of Transaction	Approximately 1800 positions filled annually	Approximately 800 positions filled annually	Approximately 200 positions filled annually	Approximately 600 positions filled annually	Approximately 500 positions filled annually
	Dollar Volumes				
Year 4	$73 million	$70 million	$19 million	$36 million	$9 million
Year 3	$68 million	$69 million	$14 million	$27 million	Implemented
Year 2	$61 million	$65 million	$13 million	Implemented	N/A
Year 1	$55 million	Implemented	Implemented	N/A	N/A

Cindy is responsible for ensuring client satisfaction and leads outreach efforts to engage Purchasing Entities and State users. Within this role, she coordinates the efforts of management, program teams and partners, ensuring a synergistic approach to client needs. She manages the full lifecycle of client engagement, including proposal development, contract negotiation and management, providing project management oversight and serving as a liaison in support of implementation and delivery teams. Cindy has direct access to the executive management team and is able to negotiate terms and conditions for changes / additions in Solution scope. She has the authority to call upon and commit resources necessary to ensure client satisfaction. She advises the State of performance under the terms and conditions of the Contract.

Below is a detailed resume for the Contract Manager, Cindy Davis.

CINDY DAVIS

Director, Government Solutions
CindyD@KnowledgeServices.com

Function and Specialization
Contract Manager, Client Engagement Management for Government Workforce Solutions

Key Responsibilities

- Key Account Management
- Program Management
- Client Relationship Management
- Contract Management
- Client Satisfaction

Education, Licenses and Certifications
Bachelor of Business Administration
Saint Mary's College, Notre Dame
2004

Background
Cindy Davis, Director of Government Solutions, is responsible for account management, contract management, business development and supporting implementation and delivery teams in the government sector. Her background includes extensive experience with State, Local and Federal government entities with a focus on developing major account management strategies. In her role, Cindy coordinates the efforts of management, dedicated Program Teams and business partners, ensuring a synergistic approach to client needs. She manages the full lifecycle of client engagement, including proposal development, contract negotiation and management, providing project management oversight and serving as a liaison in support of implementation and delivery teams.

Client Engagement Description **2013 - Present**

- Account Management for State government VMS / MSP Program with approximately $9 million in spend for administrative and light industrial
- Responsible for ensuring client satisfaction and contract management, serving as an escalation point for client executive sponsorship
- Liaison for the Implementation and Program Team with the Executive Management Team
- Active participation in weekly client status calls, hiring manager and vendor training, and regularly scheduled in person meetings with client executive sponsorship
- Participate in quarterly business reviews for client

Client Engagement Description **2015 - Present**

- Account Management for State government VMS / MSP Program with approximately $2 million in spend for IT and SOW staff augmentation, responsibilities as described above.

Client Engagement Description **2015 - Present**

- Account Management for State Government VMS / MSP Program with approximately $65 million in spend for IT Staff Augmentation, responsibilities as described above.

Past Client Engagement Description **2005 - 2012**
Professional and Industry Experience
Director, Education Services

VI. Technical Response

This section should constitute the Technical response of the proposal and must contain at least the following information:

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

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

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

Knowledge Services has read Section 8 of the RFP. Below is Knowledge Services' specific point-by-point response, in the order listed, to each requirement in that section.

Knowledge Services' assessment of the Cloud Solutions to be provided is for the Lead State (State of Utah) in cooperation with NASPO ValuePoint Cooperative Purchasing Program to establish Master Agreements for Cloud Solutions. The Cloud Solutions need to have the ability to provide efficiency, cost savings, scalability, business continuity and flexibility. The scope encompasses three service models: 1) Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Knowledge Services' SaaS Cloud Solution, dotStaff™, is a Vendor Management System (VMS), mobile case management and mobile workforce Solution providing government entities a web-based, mobile accessible platform allowing States, agencies and organizations to easily engage and govern their entire workforce management program including contingent workers, contractors and Independent Contractors (IC / 1099s), service providers and State full time employees (FTEs). The dotStaff™ Software as a Services (SaaS) platform incorporates the entire workforce engagement and oversight process, including sourcing management, assignment management, communication management, time and activity tracking, progress reporting and billing, as well as secure document sharing and advanced predictive analytics, in a user-friendly configurable application that increases efficiency, provides improved governance and accountability, reduces costs and drives compliance throughout an organization.

In serving government needs for Vendor Management, dotStaff™ addresses requirements for managing vendor-based contingent and temporary labor, fixed-bid and milestone Statement of Work (SOW) and field-based mobile and in-home service provider management. Utilizing the dotStaff™ SaaS platform, government entities are able to improve operational efficiencies, provide improved governance and accountability and improve information access of field and mobile-based workers.

The Solution's growth, overall use and acceptance has been driven by its unique and broad functionality, supported by superior, customer service oriented MSP Program services. dotStaff™ is highly configurable and, therefore, can be configured to meet and adapt to the evolving governmental demands. As governments continue to look for savings opportunities, and are constantly challenged to do more with less, validating activity around their entire workforce within a single, cloud-based platform has proven to provide significant value.

The Knowledge Services dotStaff™ Solution is the only provider in State government that supports all traditional and non-traditional contingent and temporary labor categories. dotStaff™ is also the only State government-deployed SaaS platform for the procurement, mobile case management and workforce management process that supports stationary State Full Time Employees (FTEs), State mobile FTEs, mobile contract workers, contracted vendor and service provider workers who travel from site to site or from appointment to appointment.

The Knowledge Services dotStaff™ Pro Solution provides government entities a Vendor and Contract Management System, supported, where applicable, by our Managed Service Provider (MSP) Program, that focuses on improving and facilitating the hiring process for their contingent and State FTE labor needs. Our clients benefit from one point of contact who manages, on their behalf, the entire contingent labor process from requisition and contract management to billing and invoicing to reporting and business analytics. Our Pro Solution provides State governments with hard dollar cost savings through real-time bill rate reverse auction and rate card management; improved compliance and risk mitigation through streamlined credentialing and Independent Contractor / 1099 compliance; and automated processes and approval workflows to simplify the entire contingent and State FTE workforce process.

The Knowledge Services dotStaff™ Mobile Pro Solution provides a total cost of ownership (TCO) on a single integrated platform. Our clients benefit from streamlined access to critical business intelligence (BI) allowing for informed decision making with real-time, accurate data and analytics that improve citizen outcomes and internal processes. The Mobile Pro Solution provides essential fraud prevention capabilities as well as time, date and location validation activities for the entire workforce – stationary, mobile, State FTE and contractor. Our SaaS Solution provides route optimization with an integrated calendaring and scheduling component that offers real-time alerts and notifications.

Technical Requirements (Section 8.1)

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 Knowledge Services Cloud Solution we intend to provide to Eligible Users, service model is a Software as a Service (SaaS) and the deployment model is Private Cloud.

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.

Knowledge Services understands the importance of meeting the NIST-essential characteristics. Our Cloud Solution meets the NIST Characteristic of On-Demand Self-Service because, in our Software as a Service (SaaS) environment, we are measuring usage and responding to the environment growth in advance of need. This is transparent to the end user and occurs without need of human interaction from the consumer to the provider.

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

The Knowledge Services Cloud Solution meets the NIST Characteristic of Broad Network Access because our Software as a Service (SaaS) model can be accessed over the public internet from any supported mobile device or any device running a supported web browser.

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.

The Knowledge Services Cloud Solution meets the NIST Characteristic of Resource Pooling for the reason that the provisioning of computing capabilities (storage, processing, memory and network bandwidth) is managed by the Offeror and is transparent to the consumer in our Software as a Service (SaaS) model.

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.

The Knowledge Services Cloud Solution meets the NIST Characteristic of Rapid Elasticity because the provisioning of computing capabilities (storage, processing, memory and network bandwidth) is managed by the Offeror and is transparent to the consumer in our Software as a Service (SaaS) 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.

The Knowledge Services Cloud Solution meets the NIST Characteristic of Measured Service for the reason that the provisioning of computing capabilities (storage, processing, memory and network bandwidth) is managed by the Offeror and is transparent to the consumer in our Software as a Service (SaaS) model.

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.

Knowledge Services' SaaS Solution offerings are e-procurement, workforce management and information SaaS offerings that cover areas such as Vendor Management Systems (VMS), Electronic Visit Verification (EVV), document management, mobile case management, workforce management and e-Forms.

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

Knowledge Services has read, understands and agrees 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.

Knowledge Services' Cloud Solution adheres to the services, definitions and deployment models identified in the Scope of Services, in Attachment D. Knowledge Services' Cloud Solution, dotStaff™, provides convenient, on-demand access to the cloud-based service. Our Cloud Solution has the ability to store and secure low and moderate risk data. The dotStaff™ Solution is capable of meeting the five essential characteristics which include: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. The Knowledge Services Cloud Solution that aligns with NIST requirements and standards is a Software as a Service (SaaS) that is deployed through a private cloud. Our Cloud Solution is accessible from various client devices through a supported web browser or mobile device.

Subcontractors (Section 8.2)

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 Subcontractors that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

Knowledge Services does intend to provide Cloud Solutions directly and not through the use of Subcontractors.

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.

Knowledge Services does intend to provide Cloud Solutions directly and not through the use of Subcontractors.

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.

Knowledge Services does intend to provide Cloud Solutions directly and not through the use of Subcontractors.

Working with Purchasing Entities (Section 8.3)

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.*

Knowledge Services will work with Purchasing Entities before, during and after a Data Breach. A robust network security monitoring solution is in place that leverages signature-based software and live analysts monitoring the network traffic of our organization. The false positive rate is extremely low and all events are thoroughly analyzed. In the event of an incident, the third party company alerts a local point of contact to investigate the issue. The third party provides full details regarding the event and recommended remediation steps based on the severity of the issue.

- Personnel – A local point of contact from Knowledge Services will be contacted by a third party monitoring analyst. The local point of contact from Knowledge Services will notify the Contract Manager, who will then contact Purchasing Entities' point of contact.
- Response times – The response time in the event of a Data Breach is within an hour of identification of a true positive.
- Methods of communication – The methods of communication of a Data Breach are via a portal, email and phone.

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.

Knowledge Services will not engage in or permit our agents to push adware, software or marketing not explicitly authorized by the Purchasing 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.

This is applicable to an application hosting environment that is hosting other supplier's services. This is not applicable to our SaaS Solution, as we are hosting only our service. Our team does have access to Product Environment Test and Staging.

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

Knowledge Services understands and will comply with Participating Entity's accessibility policies, as applicable.

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

The Knowledge Services Cloud Solution application and content delivered through it are accessible through latest versions of Internet Explorer, Chrome and Firefox. Our testing regiment includes validating support for the latest version of all three browsers and periodically includes back version regression testing.

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.

Knowledge Services will meet the Purchasing Entity, cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used that is subject to any law, rule or regulation providing for specific compliance obligations. As standard practice with each new program, our deployment team completes an initial findings meeting and subsequently, as needed, a discovery phase. The purpose of the findings meeting and discovery phase is to determine the configuration requirements and types of data to be stored. A report of findings and subsequent sign-off by the procuring entity, ensures that both parties are aware and agree to any security steps required to meet compliance obligations.

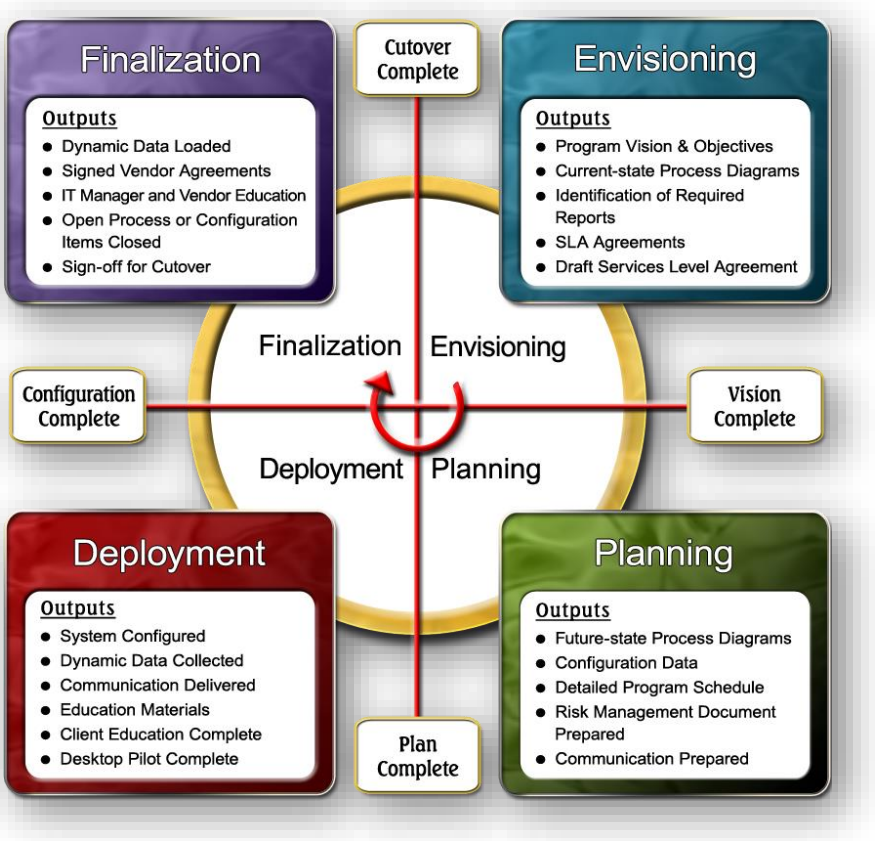
8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Knowledge Services provides a highly proven and reliable implementation. This process framework ensures objectives are accomplished with sufficient flexibility to meet unique State needs. As illustrated in the figure below, the implementation is divided into four phases:

- Envisioning – understanding State objectives, current practices
- Planning – current state process discovery and mapping, review of current processes and user guides, recommended future state process, change management plan, data collection, communication template modification, schedule development and State sign off of each of these outputs

- Deployment – communication plan execution, change management plan execution, data load, user education, desktop pilot and sign-off
- Finalization – execution of any process, data or system adjustments requested during desktop pilot

Figure



Our implementation approach focuses of the following success factors:

- 100% engagement and understanding of Solution benefits
- Accomplishment of all stated State objectives
- Succinct and effective communication to all Solution constituency
- Seamless change management execution
- On-going measurement, reporting and advising

Our Cloud Solution implementation plan is typically completed within 8 to 12 weeks. This plan also includes information, data and knowledge transfer.

The Figures on the following three pages illustrate the summarized implementation process flow, including the timing of the various steps identified in the narrative above.

Figure – Implementation Process Flow – Section 1

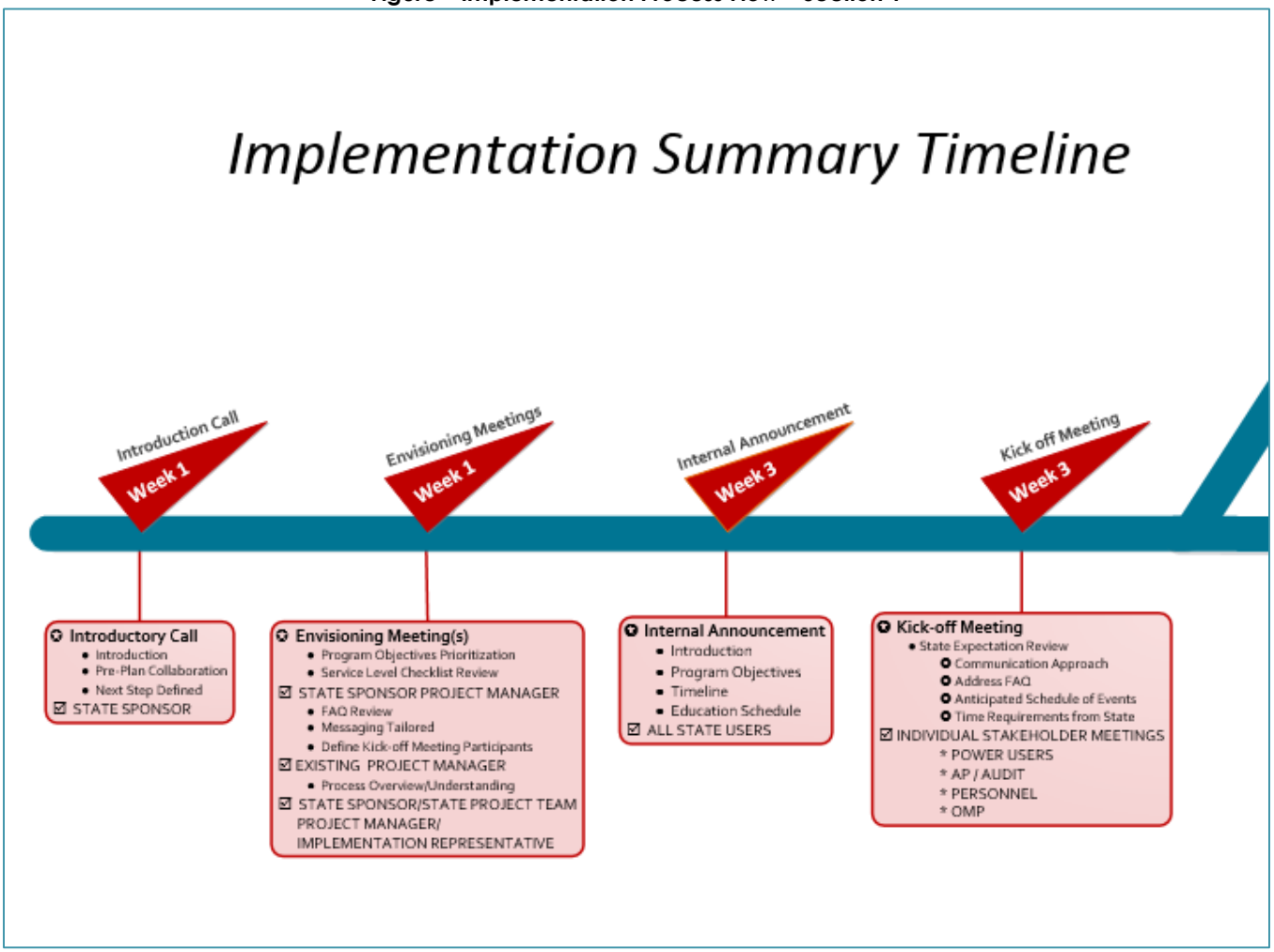


Figure – Implementation Process Flow - Overview

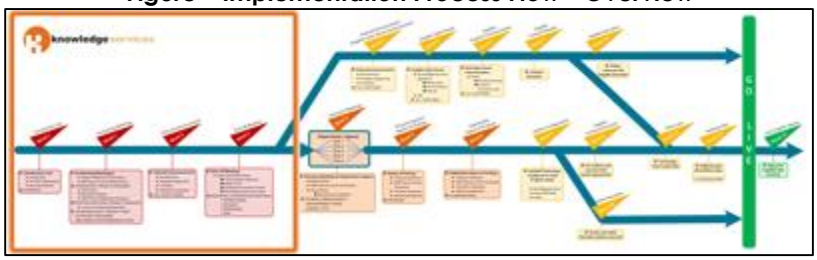


Figure – Implementation Process Flow – Section 2

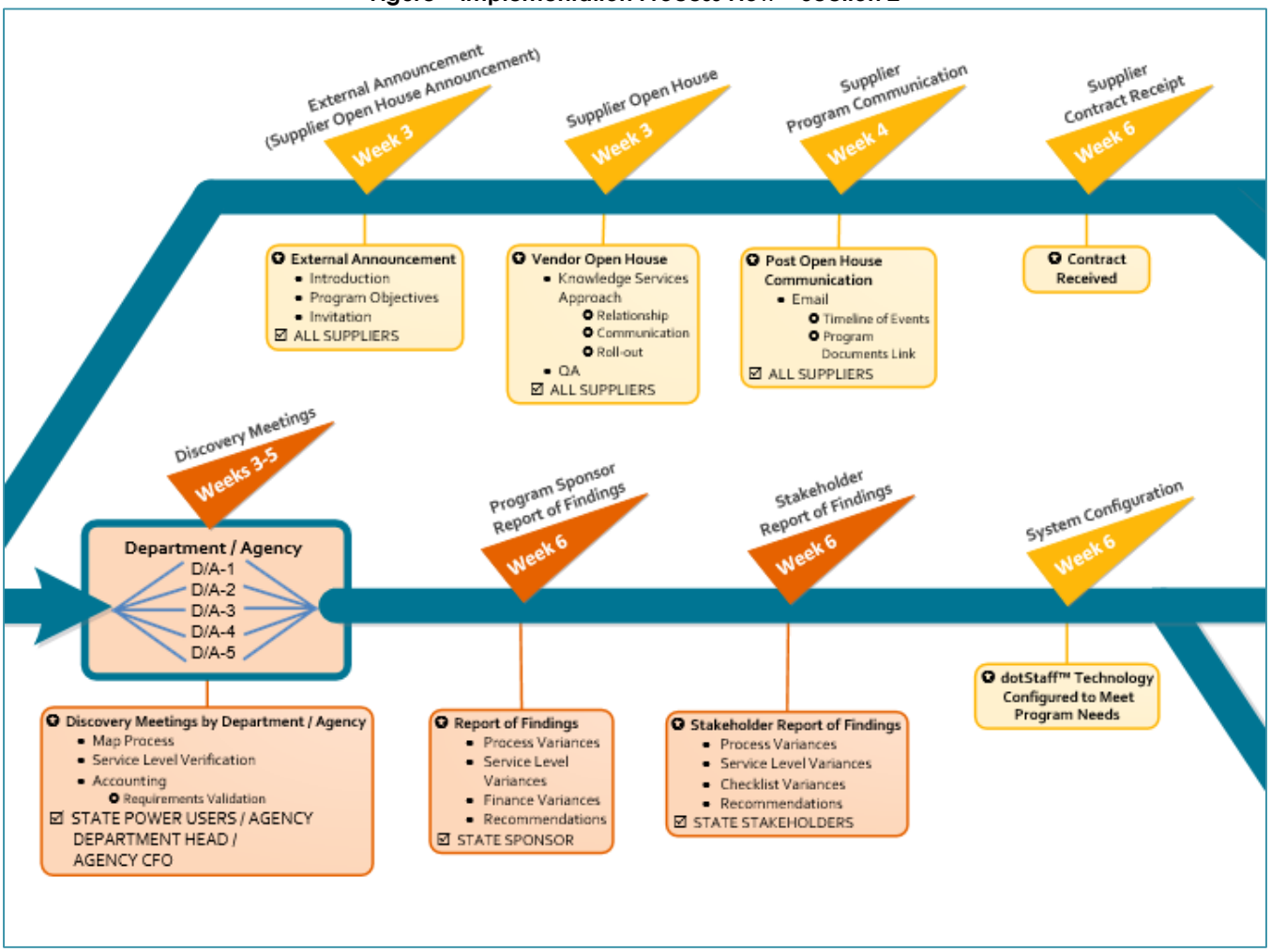


Figure – Implementation Process Flow – Overview

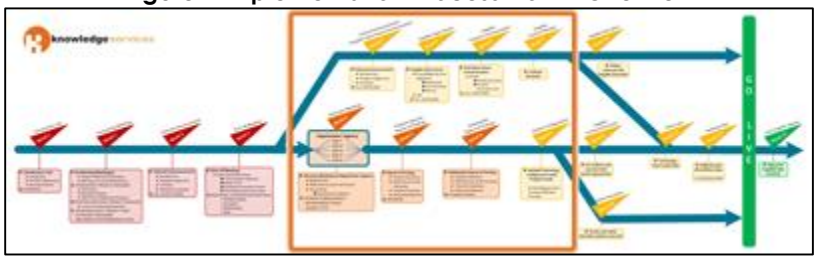


Figure – Implementation Process Flow – Section 3

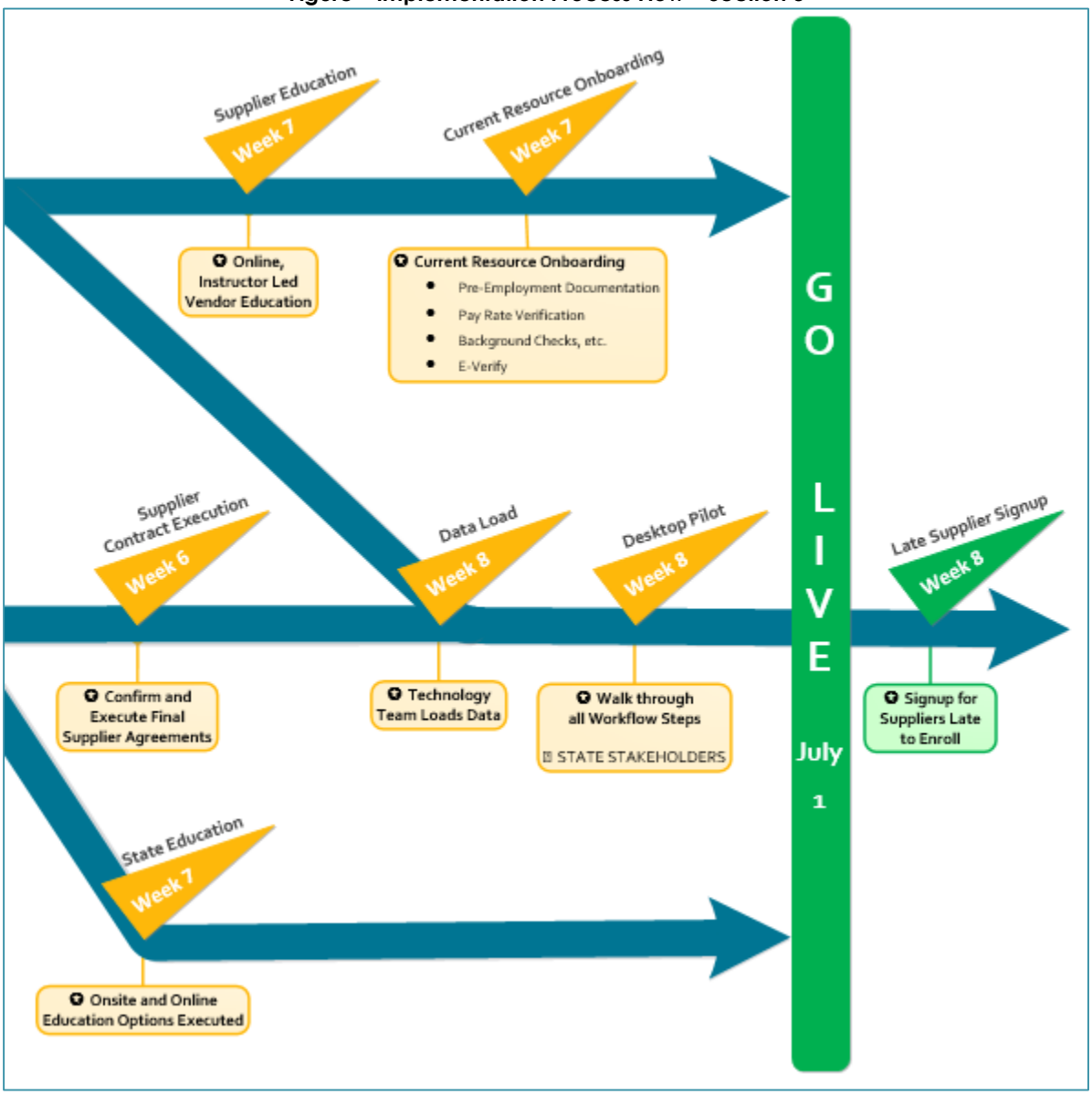
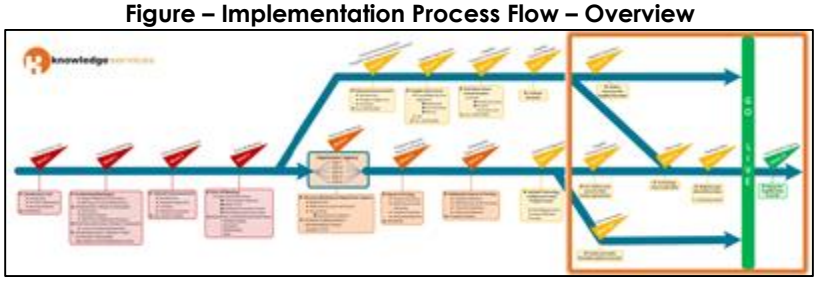


Figure – Implementation Process Flow – Overview



Knowledge Services will meet with the State to review potential technical and logistical issues of the proposed implementation plan. We will provide a finalized implementation plan based on the feedback received from the State. To ensure a timely and satisfactory implementation, Knowledge Services and the State will jointly agree to a final implementation plan. We will provide a weekly update to State stakeholders on the progress of the implementation to ensure State satisfaction.

The implementation will begin with an envisioning phase. An introductory meeting will be held to confirm and document the State's objectives. These objectives will be tracked throughout the implementation and Go-Live for purposes of measuring implementation and Program Solution success. The introductory meeting is followed by additional meetings where we, along with the State, validate project steps and make State and Agency specific adjustments to the plan.

Knowledge Services' discovery sessions will include identifying and documenting current State process mapping, systems integration needs, area-specific approval workflows and business rules and resource requirements. Knowledge Services will then develop and recommended future state processes, change management strategy and communications management plans and templates.

The State's business rules will be captured and documented during the Knowledge Services discovery meetings, presented and validated with sponsors and stakeholders during the Report of Findings meetings and incorporated into the dotStaff™ Cloud Solution during system configuration.

After acceptance of the Report of Findings to all stakeholders, the balance of the implementation tasks are completed, including:

- State user education
- Vendor / Provider network enrollment
- Vendor / Provider network education
- User education
- Technology configuration
- Data load
- Final State audit of data
- Go live

Customer Service (Section 8.4)

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

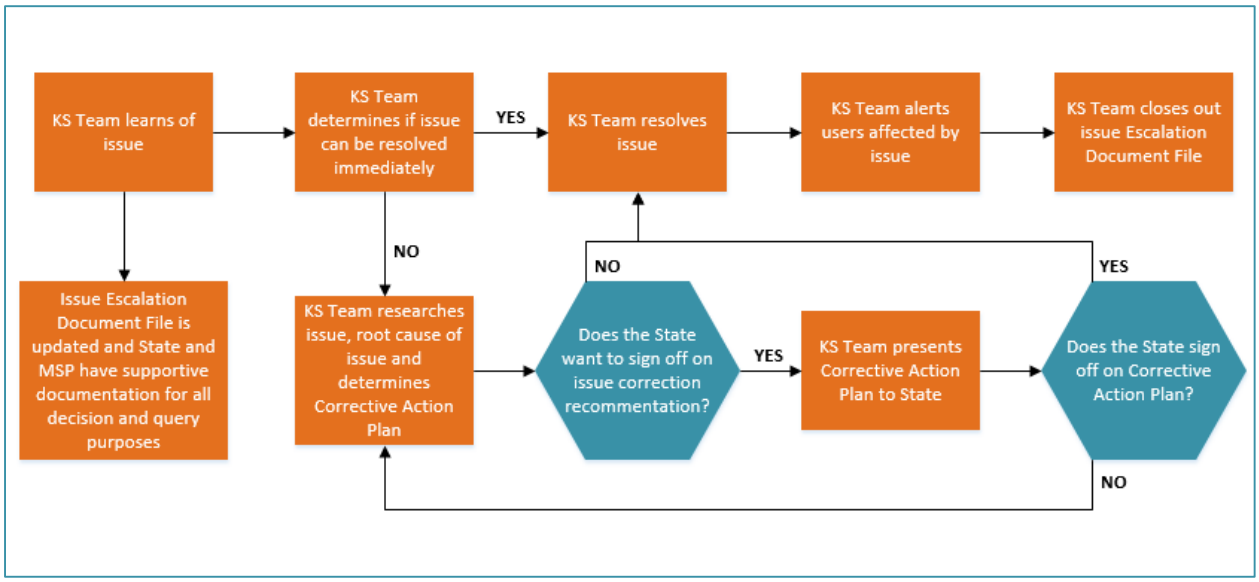
- *Quality assurance measures;*
- *Escalation plan for addressing problems and/or complaints; and*
- *Service Level Agreement (SLA).*

One of our key strengths is the ability to provide exceptional customer service, supported by detailed problem resolution and escalation procedures. We take a proactive approach to issues; therefore, we address minor problems immediately and regularly assess and re-assess our Solution and services to identify any potential difficulties to prevent need for escalations. These procedures are documented, tracked and reported on during our meetings with the State.

Knowledge Services will configure our standard escalation procedure specifically for the Purchasing Entity to include various issues that may arise throughout the Solution and meet Contract and Participating Addendum requirements. The process will be addressed, and, if required, adjusted during implementation and throughout the term of the Participating Addendum.

Knowledge Services has a clearly-defined issue management and resolution with escalation structure that begins with our dedicated Program Manager, who administers our Solution. All issues are first escalated through the manager, then triaged and assigned a priority for resolution. An issue log is maintained, and communication on the status of the resolution is provided to all involved parties. The Program Manager is able to quickly call to action any and all appropriate program and technical support and management team members, day or night, weekday or weekend, standard or holidays. As necessary, the escalation path flows directly to the Knowledge Services Executive Vice President, responsible for all Cloud Solutions.

The direct escalation path is urgency-based and can occur via email and / or by phone for critical matters, 24 x 7 x 365. Further escalation steps are in place for reaching the President and, as necessary, the company CEO. Escalations are documented and tracked and status reporting is monitored by the Knowledge Services' Executive Vice President and provided to Participating Entity management.



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

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

Knowledge Services will meet the requirement to have one lead representative for each entity who executes a Participating Addendum and contact information will be kept current. With all of our Cloud Solutions, we have a dedicated Program Manager who will serve as the lead representative for each Participating

Addendum.

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

Knowledge Services will meet the requirement to have customer service representative(s) available by phone and / or email from 7 AM to 6 PM on Monday through Sunday for the applicable time zones.

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

Knowledge Services will meet and exceed this requirement and customer service representatives will respond to inquiries within one business day.

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

Design services are not applicable for this category and our Cloud Solution.

e. You must provide Installation Services for the applicable categories.

Installation Services are not applicable for this category and our Cloud Solution.

Security of Information (Section 8.5)

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.

Knowledge Services understands the importance of protecting data; we employ the following security measures to do so.

Server Backup Strategy

- Server Baselines taken and stored in backup appliance
- CDP (Continuous Data Protection) takes differences once an hour on production servers
- Backups are synced with off-site storage as they occur
- Monthly Backups are retained for one year and then rolled in to annual backups which are kept for seven years.

Database Backup Strategy

- Production Databases set to full recovery mode

- Transaction Logs are backed up every 15 minutes
- Full database backups taken nightly
- Log files and database backups synced to off-site storage every 15 minutes
- Full point in time recovery retained for 90 days
- Full database backup retention rate via the server backup strategy

Other Security Considerations

dotStaff™ has a security committee dedicated to the protection of the application and data assets of dotStaff™ and our clients. This committee constantly reviews security requirements against current practice to determine additional actions that may be warranted, or new technologies that can be employed.

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

Knowledge Services intends to comply with all applicable laws and related data privacy and security by utilizing our information security program based on NIST 800-53 with a focus on HIPAA security and privacy. A robust network security monitoring solution is in place, along with a proactive vulnerability management program. Applicable policies and procedures are in place that support the security and privacy program. A cycled approach to risk assessment and management is in place that hinges on a holistic risk assessment and prioritized remediation cycle.

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.

Knowledge Services will not access the 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. As a matter of policy, client data is not reviewed or accessed except in situations of technical support and at the request of the client. Records are kept of technical inquiries and remedies. Records include data / time stamp, support representative identification and status information. For purposes of performance testing, client data may be used. Data obfuscation is deployed to ensure confidentiality.

Privacy and Security (Section 8.6)

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.

Knowledge Services is committed to complying with NIST and other relevant industry standards. Our security program is aligned with NIST 800-53 and HIPAA. The risk assessment and management program is on a cycle of analysis, prioritization, remediation and reanalysis.

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.

The government or standards organization security certifications Knowledge Services' Cloud Solution's security program is aligned with NIST 800-53 and HIPAA. The risk assessment and management program is on a cycle of analysis, prioritization, remediation and reanalysis. Offeror also holds a certification for ISO 27001.

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.

Knowledge Services has 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 Knowledge Services information security program is based on NIST 800-53 with a focus on HIPAA security and privacy. A robust network security monitoring solution is in place, along with proactive vulnerability management program. Applicable policies and procedures are in place that support the security and privacy program. A cycled approach to risk assessment and management is in place that hinges on a holistic risk assessment and prioritized remediation cycle.

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.).

Knowledge Services meets the requirement to have data confidentiality standards and practices in place to ensure data confidentiality. We have Confidential and Mobile Data Policies which are provided in the Appendix to this RFP response (ISP-005 and ISP-006) and ensure comprehensive coverage of confidential information on mobile hardware.

The purpose of our Confidential Data Policy is to detail how to identify and handle confidential data. This policy lays out standards for the classification and use of confidential data, and outlines specific security controls to protect this data.

The purpose of our Mobile Device Policy is to specify company standards for the use and security of mobile devices.

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

Knowledge Services' third-party attestations, reports, security credentials and certifications relating to data security, integrity and other controls include:

- ISO 27001
- 9001 Compliance

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.

Knowledge Services has described below our logging process, including the type of services and devices logged, the event types logged and the information fields.

Knowledge Services' information security program is based on NIST 800-53 with a focus on HIPAA security and privacy. A robust network security monitoring solution is in place, along with a proactive vulnerability management program. Applicable policies and procedures are in place that support the security and privacy program. A cycled approach to risk assessment and management is in place that hinges on a holistic risk assessment and prioritized remediation cycle.

The logging of events is an important component. Logs contained on application servers, network devices and critical systems may all contain different data, but all contain valuable information that the Company must record. Thus, the Company requires that logging on network-level devices must be enabled to the fullest degree possible. Passwords must not be contained in the logs.

Audit trails are similar to logging, and typically are created from logs, but differ in that audit trails are typically chronological and designed to allow for the reconstruction and examination of the activities surrounding network and system events.

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

Knowledge Services meets the requirement to restrict visibility of cloud-hosted data and documents to specific users and / or groups. With multiple State governments, the dotStaff™ Solution was designed with configuration controls which can be conformed to each State agency's needs, at no additional cost to the State. The dotStaff™ Solution is configurable to support multiple State user groups as well as multiple user roles according to access to necessary data and functionality.

The dotStaff™ Solution meets this requirement through its role-based security model. Roles include: dotStaff™ Administrator, Client Administrator, Client User, Vendor / Provider Administrator, Vendor / Provider User, Resource and MSP, with the ability to include additional user roles such as patient, caregiver and guardian. The configuration options in the dotStaff™ VMS allow one to assign "view" and "edit" access to a specified subset or group of roles, enabling rights to perform various functions as needed. All users must be authenticated before gaining access to the dotStaff™ Solution. Once authenticated by username and encrypted password, specific application roles are used to grant access to specific data by specific role types. Form and field-based security can also be identified in specified user areas within the dotStaff™ Solution.

The security levels inherent in dotStaff™ are illustrated in the figure, Security Overview, below.

Figure – Security Overview

Role	Postings/Requisitions	Submissions	E-Contracts	Time Sheets / Expenses	Invoices	Reports
dotStaff Administrator	ECA	ECA	ECA	ECA	ECA	ECA
MSP	ECA	CE	CE	CE	View	CE
Client Administrator	ECA	View	View	ECA	View	CE*
Client User	ECA	View	View	ECA	View	CE
Vendor Administrator	View	CE	View	CE	View	CE
Vendor User	View	CE	View	CE	View	CE
Resource	None	None	None	CE	None	View (Time Report only)
Key						
None	No Access					
View	View only					
CE	Create, Edit, and View					
ECA	View Edit and Approve					
Note:	Throughout the dotStaff Technology, individuals can view only items created by them, by the MSP on their behalf, or items they are granted access to view by the creator of the document					

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.

Knowledge Services meets the requirement for a notification process in the event of a security incident, including relating to timing and incident levels. Knowledge Services understands and will comply with the

requirement that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

A robust network security monitoring solution is in place that leverages signature based-software and live analysts monitoring the network traffic of our organization. The false positive rate is extremely low and all events are thoroughly analyzed. In the event of an incident, the third party company alerts a local point of contact to investigate the issue. The third party provides full details regarding the event and recommended remediation steps based on the severity of the issue.

- Personnel – A local point of contact from Knowledge Services will be contacted by third party monitoring analyst. The local point of contact from Knowledge Services will notify the Contract Manager, who will then contact Purchasing Entity's point of contact.
- Response times – The response time in the event of a data breach is within an hour of identification of a true positive.
- Methods of communication – The methods of communication of a data breach are via a portal, email and phone.

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.

Knowledge Services meets the requirement to have security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers. Traffic is filtered through an IPS / IDS system to Cisco ASA firewalls. Servers are logically separated into VLANs appropriate to their function. Traffic is managed via firewall rules and ACLs. All traffic is blocked or dropped from untrusted networks except for specified firewall exceptions to servers residing in the DMZ.

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).

Knowledge Services has provided our technology architecture that supports our Software as a Service (SaaS) Solution; please refer to Appendix – dotStaff™ Technology Architecture.

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.

Knowledge Services meets the requirement for security procedures in place regarding our employees who have access to sensitive data. We believe good security starts with good user security, thus we require that potential personnel be screened prior to hire. The level of screening should be appropriate to the position, with more in-depth background checks required for personnel with greater responsibilities or access to confidential information and / or ePHI. Examples of acceptable screening methods include checking employment history, criminal records, credit history and reference checks.

We institute screening procedures for all members of the workforce who will have access to ePHI. This must include some or all of the following:

- Reference checking
- Background checking
- Credit checking
- Confirmation of experience
- Confirmation of qualifications
- Confirmation of licenses / certifications (as appropriate to position)

The logging of events is an important component. Logs contained on application servers, network devices and critical systems may all contain different data, but all contain valuable information that the Company must record. Thus, the Company requires that logging on network-level devices must be enabled to the fullest degree possible. Passwords must not be contained in the logs.

Audit trails are similar to logging, and typically are created from logs, but differ in that audit trails are typically chronological and designed to allow for the reconstruction and examination of the activities surrounding network and system events.

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.

The dotStaff™ Solution encrypts data in transit via a 2048bit SSL certificate over HTTPs. Data elements that require encryption at rest are encrypted using an MD5 cryptographic hash.

Knowledge Services Solution information security program is based on NIST 800-53 with a focus on HIPAA security and privacy. A robust network security monitoring solution is in place, along with a proactive vulnerability management program. Applicable policies and procedures are in place that support the security and privacy program.

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

Knowledge Services meets the requirement for a notification process in the event of a security incident, including relating to timing and incident levels. Knowledge Services understands and will comply with the requirement that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

A robust network security monitoring solution is in place that leverages signature based software and live analysts monitoring the network traffic of our organization. The false positive rate is extremely low and all events are thoroughly analyzed. In the event of an incident, the third party company alerts a local point of contact to investigate the issue. The third party provides full details regarding the event and recommended remediation steps based on the severity of the issue.

- Personnel – A local point of contact from Knowledge Services will be contacted by third

party monitoring analyst. The local point of contact from Knowledge Services will notify the Contract Manager which will then contact Purchasing Entities point of contact.

- Response times – The response time in the event of a data breach is within an hour of identification of a true positive.
- Methods of communication – The methods of communication of a data breach are via a portal, email and phone.

Migration and Redeployment Plan (Section 8.7)

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.

In the event that service to a Purchasing Entity will be closed down, the Purchasing Entity will define the close down requirements via a formal transition interview. During this communication, the Purchasing Entity will answer questions that will frame the close down process that will be meet their needs. The following will be identified:

- Data Transport
  - Will the data be exported for use by a subsequent provider
  - What format will best support the transition effort: XML, Excel, etc.
  - Will data export include only metadata (user lists, contracts, bill rates, etc.) or include historical data (timesheets for users, expenses for users, etc.)

- Data Protection
  - Will data remain in our data stores under standard security protocol until:
    - Conversion is complete
    - On continuous basis for historical access upon request by Purchasing Entity

- Cutover Timing
  - What is the required access timeframe by Purchasing Entity identified personnel for accessing data after closed down
  - What is the final date for time entry, invoicing, etc.

Closedown Process

Upon completion of the close down framework, the Product Service team will set contract end effective dates so that when the date is reached, all contracts in the system will be Ended and no further entries can be made. Subsequent to this, a full backup of data will be made and stored as requested by Purchasing Entity. Data cleansing will occur as directed by the Purchasing Entity and as required, will be maintained under standard security measures.

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.

All data contained within the dotStaff™ Solution is available 24 x 7 x 365 from within the dotStaff™ reporting engine. The Purchasing Entity may also request and dotStaff™ will provide a complete data export and / or file transfer within a commonly accepted file format. Availability is not limited to contract termination or expiration. Additionally, the comprehensive Purchasing Entity Program Configuration, Operations, Policies and Procedures manual, which will be developed by Knowledge Services during Implementation to include all Purchasing Entity approved State process maps, change and communications management documents and procedures, communications templates, agency-specific requirements, cloud solution configurations, communications, etc., will also be available to Purchasing Entity throughout the contract duration and, as applicable, at contract expiration and / or termination.

Service or Data Recovery (Section 8.8)

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).

Multiple types of downtime are recognized and measured for service or data recovery. Planned down time can be due to product upgrades and / or maintenance patches. These are performed on regular cycles with appropriate advanced communication to our user base. During these routine outages, although risk is low, the team is prepared with risk mitigation steps should the outage be extended for unplanned reasons. Standard protocol is to ensure proper backup and communication strategies are in place should this occur.

Unplanned outages, initiate plans that include review / discovery, impact assessment, communication, corrective action, and postmortem review. In the case of an unplanned outage, recovery team is notified via monitoring or call center teams. The recovery team, is prepared with point of contact information for communication which initiates the 'Lead Team' which is responsible for all communication regarding the outage, impact, status and any specific client communication required. The recovery team is charged with reviewing circumstances and determining required corrective action.

Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security policy. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers or malicious users; or physical risks such as loss / theft of a device, hardware failure, fire or natural disaster. Protecting critical and confidential data and key systems from these risks is of paramount importance to Knowledge Services. An Incident Response Policy is not effective at managing risk if it is not maintained and kept current, thus our policy is reviewed and tested at least annually.

In the event of an extended outage, a number of activities are initiated. Upon notification from within our technology, team or from a user, the Information Technology Team would assess the specific issues to determine cause and the extent of impact.

Knowledge Services has a formal communication plan that is executed by our 'Lead Team'. The 'Lead Team' is the team responsible for managing all product delivery activities and all communications to Purchasing Entities and users relating to planned or unplanned down time. This group allows us to continue regular communication updates without impact to our Technology Team who are assigned to resolution activities.

Knowledge Services' SaaS Solution provides access to users for (some) time sensitive activities and for each of the mission critical, time sensitive data entry requirements, a specified backup plan is deployed via the Program Manager. A Program Manager is assigned to each client and are dedicated to immediate response during day to day activities. In a 'down' instance projected to remain dawn for a period of time, the Program Manager would execute these backup options and would do so at the direction of the 'Lead Team'. One such example would be the communication to use a paper time sheet until such time that the service was rendered available once again.

Knowledge Services' monitors uptime and has met in excess of 99.5% uptime over the last 10 years while serving State government. Our monitoring tools and failover options minimize risk of extended downtime.

If we have an unrecoverable loss of data outside the RPO and RTO times, we would work with our 'Lead Team' to communicate with the Purchasing Entities what may have been lost during that time and next steps to recover or enter any lost data.

Every component powering the dotStaff™ product is built with minimum N+1 redundancy in mind from the power supplies in each server to the data center itself.

- Redundant A / B power feeds backed by battery backup and diesel generators
- Redundant Multi-Carrier Internet Connections
- Best in class Dell Servers built with redundant power supplies and redundant network connections to our Cisco switch stack
- Redundant Cisco Switches, Cisco ASA Firewalls, Cisco IPS / IDS system and redundant Citrix VPX load balancers
- Redundant data centers: primary data center in Carmel, Indiana and secondary data center in Memphis, Tennessee

Beyond building high availability across the dotStaff infrastructure, our backup and recovery plans support restoring the dotStaff system within four hours should we suffer a severe system outage. Our backup strategy, and RPO / RTO objectives are outlined below.

Server Backup Strategy

- Server Baselines taken and stored in backup appliance
- CDP (Continuous Data Protection) takes differences once an hour on production servers
- Backups are synced with off-site storage as they occur

- Monthly Backups are retained for one year and then rolled in to annual backups which are kept for seven years.

Database Backup Strategy

- Production Databases set to full recovery mode
- Transaction Logs are backed up every 15 minutes
- Full database backups taken nightly
- Log files and database backups synced to off-site storage every 15 minutes
- Full point in time recovery retained for 90 days
- Full database backup retention rate via the server backup strategy

Knowledge Services' Cloud Solution Recovery Point Objective (RPO) is 15 minutes and Recovery Time Objective (RTO) is four hours.

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.

Knowledge Services' Cloud Solution methods of data backups include log files backed up every 15 minutes, full database backups every night and log files and database backups synced to off-site storage every 15 minutes.

Knowledge Services' Cloud Solution's method of server image backup includes baselines taken and stored in backup appliance. Continuous data protection takes differences once an hour for production servers. Backups are synced with off-site storage as they occur.

Knowledge Services' Cloud Solution for digital location of backup storage is our corporate office data center.

Knowledge Services' Cloud Solution's alternate data center for primary data center within the continental United States is in Memphis, TN.

Data Protection (Section 8.9)

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.

The Knowledge Services Solution, dotStaff™, encrypts data in transit via a 2048bit SSL certificate over HTTPs. Data elements that require encryption at rest are encrypted using an MD5 cryptographic hash.

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.

Knowledge Services is willing to review and potentially sign, after review and approval, any relevant and applicable Business Associate Agreements or any other agreements that may be necessary to protect data with 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.

Knowledge Services agrees to comply and meet the requirement to only use data for purposes defined in the Master Agreement, participating addendum or related service level agreement. Knowledge Services will not use the government data or government-related data for any other purpose, including but not limited to data mining. Knowledge Services agrees to comply and meet the requirement to not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Knowledge Services will not access the 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. As a matter of policy, client data is not reviewed or accessed except in situations of technical support and at the request of the client. Records are kept of technical inquiries and remedies. Records include data / time stamp, support representative identification and status information. For purposes of performance testing, client data may be used. Data obfuscation is deployed to ensure confidentiality.

Service Level Agreements (Section 8.10)

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.

Knowledge Services sample Service Level Agreement is negotiable.

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.

Knowledge Services has provided a sample below of our Service Level Agreement, which defines the performance and other operating parameters within the infrastructure operates to meet IT System and Purchasing Entity's requirements.

Service Level Agreement ("SLA")

This document outlines the service levels to be provided in the delivery of SaaS. It also provides service delivery parameters, against which the delivery of SaaS will be evaluated. The SLA provides certain rights and remedies in the event that the Customer experiences service interruption as a result of failure of dotStaff™ infrastructure.

Service uptime commitment

THIS SERVICE LEVEL AGREEMENT ("Agreement" or "SLA") shall apply to all Services provided by dotStaff™ expressly as an addendum to the Terms of Service ("TOS") for each customer / client / vendor / end user ("USER"). dotStaff™ is committed to providing a highly available and secure service to support its USERs. Providing the USER with consistent access to dotStaff™ Services is a high priority for dotStaff™ and is the basis for its commitment in the form of a SLA. The SLA provides certain rights and remedies in the event that the USER experiences service interruption as a result of failure of dotStaff™ infrastructure. The overall service availability metric is 99.9%, measured on a monthly basis.

This Service Level Agreement shall only become applicable to dotStaff™ Services upon the later of (a) completion of the "implementation period," as such term is defined in the Statement of Work (if any), or (b) ninety (90) days from contract effective date.

1. Term Definitions

Available or Availability
When the USER who's account is active and enabled has reasonable access to services provided by dotStaff™, subject to the exclusions defined in Downtime Minutes below.

Total Monthly Minutes
The number of days in the month multiplied by 1,440 minutes per day.

Maintenance Time
The time period during which dotStaff™ Service may not be available each month so that dotStaff™ can perform routine maintenance to maximize performance, is on an as needed basis.

Downtime
The total number of minutes that the USER cannot access the dotStaff™ Service. The calculation of Downtime Minutes excludes time that the USER is unable to access dotStaff™ Services due to any of the following:

i. Maintenance Time
ii. USER's own Internet service provider
iii. Force Majeure event
iv. Any systemic Internet failures
v. Enhanced Services
vi. Any failure in the USER's own hardware, software or Network connection
vii. USER's bandwidth restrictions
viii. USER's acts or omissions
ix. Anything outside of the direct control of dotStaff™

2. dotStaff Maintenance

Maintenance Notices
dotStaff™ will communicate the date and time that dotStaff™ intends to make dotStaff™ Services un-Available via the front page of the dotStaff™ product web site at least forty-eight (48) hours in advance (or longer if practical). The USER understands and agrees that there may be instances where dotStaff™ needs to interrupt dotStaff™ Services without notice in order to protect the integrity of dotStaff™ Services due to security issues, virus attacks, spam issues or other unforeseen circumstances. Below are the Maintenance Windows and their definitions:

Emergency Maintenance
These change controls happen immediately with little notification ahead of time.

Preventative Maintenance
These change controls are when we detect an item in the environment that we need to take action on, to avoid emergency change controls in the future. These change controls, if possible, will usually occur during our planned maintenance window. If this is not possible, they will occur in low peak hours with peak being defined by our network metrics.

Planned Maintenance
These are change control's being done to:

Support on-going product and operational projects to ensure optimal performance
Deploy non-critical service packs or patches.
Periodic redundancy testing.

Where possible planned maintenance will be posted 5-days prior; however, certain circumstances may preclude us from doing so. Planned maintenance windows are Saturday mornings between 8:00am and 12:00pm EST.

3. Measurement

dotStaff™ uses a proprietary system to measure whether dotStaff™ Services are Available and the USER agree that this system will be the sole basis for resolution of any dispute that may arise between the USER and dotStaff™ regarding this Service Level Agreement.

Availability is calculated based on the following formula:
A = (T – M – D) / (T – M) x 100%
A = Availability
T = Total Monthly Minutes
M = Maintenance Time
D = Downtime

4. Software-as-a-Service Credits

Financial Consequences for Non-Performance
Measured Enterprise-wide per month based on minimum performance target (not occurrence)
Maximum credit amount is $500 per month per contract.

Quarterly SaaS rating	Rating	SaaS service credit
Between 99.9% - 100%	Meets Goal	
Between 99.0% - 99.8%	Tolerable	$150 / month
Below 99.0%	Unacceptable	$500 / month

5. User Responsibility

Minimum Requirements
The required configurations USER must have to access dotStaff™ Services include:

Internet connection with adequate bandwidth
Supported Internet Browser

Remedy and Procedure
The USER's remedy and the procedure for obtaining the USER's remedy in the event that dotStaff™ fails to meet the Service level metrics set forth above are as follows:

To qualify for remedy
(a) There must be a support ticket documenting the event within 24 hours of the service interruption
(b) USER account must be in good standing with all invoices paid and up to date

The USER must notify dotStaff™ in writing within five (5) business days by opening a support ticket and providing the following details:

Subject of email must be: "Claim Notice – dotStaff™ Service Downtime"
List the type of Service that was affected
List the date the Downtime Minutes occurred
List user(s) Login Name and E-mail address affected by Downtime Minutes
List an estimate of the amount of actual Downtime Minutes
Ticket number of the documented event

dotStaff™ will confirm the information provided in the Claim Notice within ten (10) business days of receipt of the Claim Notice. If dotStaff™ cannot confirm the Downtime Minutes, then the USER and dotStaff™ agree to refer the matter to executives at each party for resolution. If dotStaff™ confirms that dotStaff™ is out of compliance with this Service Level Agreement, the USER will receive the amount of Service Level Credits set forth above for the affected Service level metric for the affected month. The SLA credit will be reflected in the dotStaff™ invoice to the USER in the invoice cycle following dotStaff™ confirmation of the Downtime Minutes. Please note that SLA credits can only be applied to accounts that are in good standing with all invoices paid and up to date.

Data Disposal (Section 8.11)

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

Knowledge Services meets the requirement to have data disposal procedures, policies and processes. Data destruction is a critical component of a data retention policy. When the retention timeframe expires, Knowledge Services actively destroys the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term implications, exceptions will be approved only by executive management.

Knowledge Services specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or company policy. Further, any data that may be subject to a subpoena or discovery request must not be destroyed.

Knowledge Services must create and follow a process that, on a quarterly basis, seeks out and securely deletes any ePHI that exceeds retention requirements defined in this policy. This process can be either automated or performed manually.

Media containing confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper / documents: cross-cut shredding or incineration is required in order to make the data unrecoverable
- All removable media such as flash drives, memory cards or CD / DVDs containing confidential data should be sent to the IT Help Desk for secure deletion or destruction
- Hard Drives / Systems / Mobile Storage Media: The strongest commercially available data wiping technology must be used to ensure that the data is unrecoverable. Data on all hard drives will be eradicated using a 7-pass system that meets or exceeds DOD standards. Alternatively, physical destruction, such that the data storage mechanism is completely destroyed, is an option. A Certificate of Destruction that contains, at a minimum, system serial number, hard drive serial number and date of destruction must be provided by the vendor and kept on file.

Media awaiting destruction under this policy must be physically secured until the necessary destruction can take place. This can be in the form of a locked cabinet or other secure storage solution.

Performance Measures and Reporting (Section 8.12)

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.

Knowledge Services has the ability to guarantee reliability and uptime 99.9% or greater availability. Every component powering the dotStaff™ product is built with minimum N+1 redundancy in mind from the power supplies in each server to the data center itself.

- Redundant A / B power feeds backed by battery backup and diesel generators
- Redundant Multi-Carrier Internet Connections

- Best in class Dell Servers built with redundant power supplies and redundant network connections to our Cisco switch stack
- Redundant Cisco Switches, Cisco ASA Firewalls, Cisco IPS / IDS system and redundant Citrix VPX load balancers
- Redundant data centers: primary data center in Carmel, Indiana and secondary data center in Memphis, Tennessee

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

Knowledge Services meets the requirement to provide standard uptime service and related Service Level Agreement (SLA) criteria. Uptime or availability as described in the SLA is, "When the USER whose account is active and enabled has reasonable access to services provided by dotStaff™," excluding downtime minutes as described in our SLA example.

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.

Knowledge Services will provide a support team that is accessible 24 x 7 x 365 via online chat, phone support or email. All inquiries are vetted immediately and resolved via our technical support team or, when applicable, escalated to additional support avenues.

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

Our Solution is a SaaS model; therefore, if we fail to meet incident response time and incident fix time, it will affect the uptime / availability. This is defined in our SLAs.

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

Knowledge Services' procedures and schedules for any planned downtime are listed below.

<u>Maintenance Notices</u>
Offeror will communicate the date and time that Offeror intends to make services un-available via the front page of the product web site at least 48 hours in advance (or longer if practical). The USER understands and agrees that there may be instances where Offeror needs to interrupt services without notice in order to protect the integrity of services due to security issues, virus attacks, spam issues or other unforeseen circumstances. Below are the maintenance windows and their definitions:

<u>Emergency Maintenance</u>
These change controls happen immediately with little notification ahead of time.

Preventative Maintenance

These change controls are when we detect an item in the environment that we need to take action on to avoid emergency change controls in the future. These change controls, if possible, will usually occur during our planned maintenance window. If this is not possible, they will occur in low peak hours with peak being defined by our network metrics.

Planned Maintenance

These are change controls being done to:

- Support on-going product and operational projects to ensure optimal performance
- Deploy non-critical service packs or patches
- Periodic redundancy testing

When possible, planned maintenance will be posted five days prior; however, certain circumstances may preclude us from doing so. Planned maintenance windows are Saturday mornings between 8:00 AM and 12:00 PM Eastern Standard Time.

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

Our Solution is a SaaS model. If a disaster occurs, there is a negative impact to uptime / availability to users, which is part of our SLA example.

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.

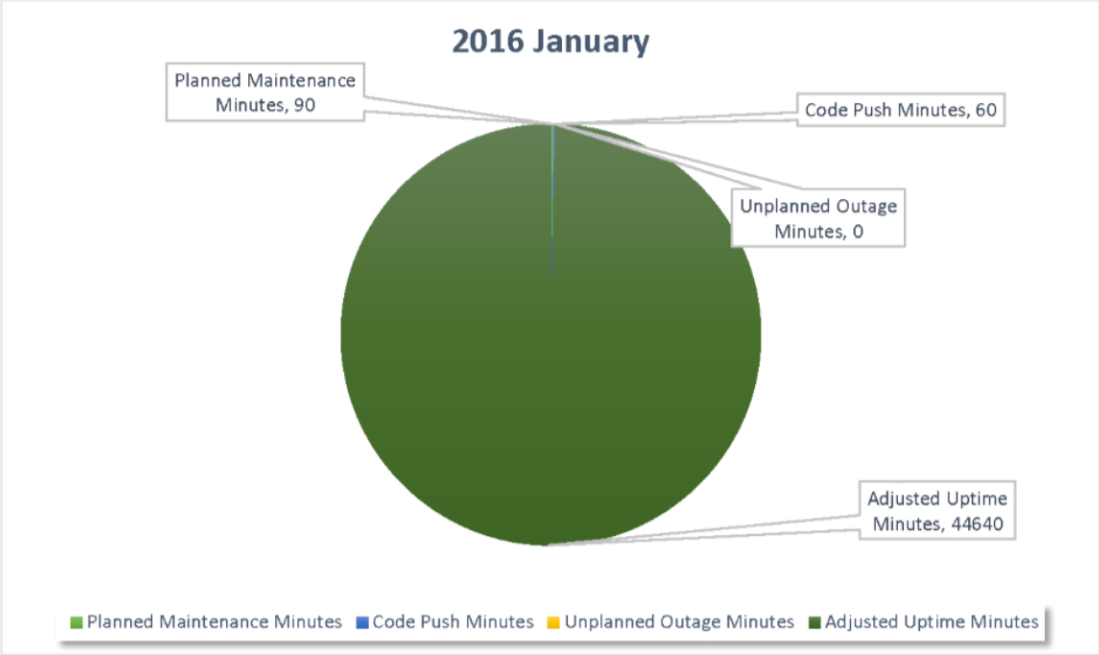
Knowledge Services will provide performance and availability reports upon request from the Purchasing Entity. The statistics are batch. In the Figure below is a sample of our performance report, which is available upon request.

Figure – Sample Performance Report

dotStaff January 2016 Uptime and Availability Report

Total Minutes for month:	44640
Planned Maintenance Minutes:	90
Code Push Minutes:	60
Unplanned Outage Minutes:	0
Total Uptime Minutes:	44490
Adjusted Uptime Minutes:	44640

January 2016 Uptime
100.000%



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

Knowledge Services complies with this requirement and has the ability to print historical, statistical and usage reports locally for information stored in the Cloud Solution.

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

Knowledge Services' SaaS Solution's underlying cloud infrastructure is supported 24 x 365.

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

Knowledge Services' SaaS Solution's underlying cloud infrastructure is supported 24 x 365.

Cloud Security Alliance (Section 8.13)

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

a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3.

Knowledge Services has completed the CSA STAR Self-Assessment, as described in Section 5.5.3.

b. Completion of Exhibits 1 and 2 to Attachment B.

Knowledge Services has completed Exhibits 1 and 2 to Attachment B and attached both as part of our RFP response.

c. Completion of a CSA STAR Attestation, Certification, or Assessment.

Knowledge Services has completed the CSA STAR Attestation, Certification, or Assessment.

d. Completion CSA STAR Continuous Monitoring.

Knowledge Services has completed the CSA STAR Continuous Monitoring.

Service Provisioning (Section 8.14)

8.14. 1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

Knowledge Services' dotStaff™ technology is capable of being implemented in timeframes commensurate with environment and complexity. Generally, there are three types of implementation scenarios that are defined below with implementation details and timeline for each:

- New User – New users can be added by the client or by our Program Team. In either case the addition of users is a single data entry activity in an existing instance of the Solution and can be complete in minutes. Such a request to Knowledge Services is completed in under two hours.

- Provisioning for other Purchasing Entities / Cooperatives – These instances are often requested with short notice and with need for immediate implementation. In these

instances, we utilize a standard implementation template to obtain appropriate configuration information and upon completion of the form, configuration of the product and data load is executed and completed within 2 - 3 business days. The supporting agreement will minimize the variables that can be set, but allows the organization to quickly engage and make use of the Solution. The 'pre-defined' configuration is intended for rapid deployment and can be adjusted overtime to optimize the Solution to client needs.

- Enterprise Wide Deployment – Generally enterprise-wide deployment begins with an introductory meeting to define goals and objectives of the procuring party. A series of discovery meetings allow our implementation team to better understand the processes and existing needs of the organization. At the conclusion of the discovery phase, a report of findings with Solution and Program configuration recommendations is provided to the organization. Upon approval, the system configuration and data load are complete. Once the system is configured, a 'Desktop Pilot' is performed, allowing the organization to walk through the entire process to ensure all requirements are met. Upon sign off of the Desktop Pilot, a go-live date is confirmed and education of client and vendor users will occur. This full implementation process is generally 8 to 12 weeks in duration for complex enterprise environments.

- A hybrid of the Purchasing Entity / Cooperative template and the enterprise-wide implementation may occur when time constraints require a shorter implementation in a complex environment.

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

Knowledge Services' dotStaff™ technology is capable of being implemented in timeframes commensurate with environment and complexity. There are three types of implementation scenarios defined in 8.14.1 above and lead time for provisioning of each is described below:

- New User – No lead time is required for provisioning a new user. The client is able to add users on demand or if client desires, they can call our Program Manager and the user will be setup during the duration of the inbound call.

- Provisioning for other Purchasing Entities / Cooperatives – A template configuration for urgent needs can be completed in two business days with a call to the Program Manager. One day lead time is sufficient.

- Enterprise Wide Deployment – Enterprise wide implementations with process discovery and configuration recommendations are generally begun within three days from date of contract sign.

- A hybrid of the Purchasing Entity / Cooperative template implementation and the enterprise-wide implementation may occur when time constraints require a shorter

implementation in a complex environment. In the event of a hybrid model, the initial configuration will be completed in two business days with one day lead time notice.

Back Up and Disaster Plan (Section 8.15)

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

Knowledge Services is able to manage legal retention periods and disposition at the client level. Where required, agencies can be treated as independent clients should they have specific legal requirements that require it.

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

We do not have inherent risks other than those that are normally anticipated. Disaster Recovery and Contingency Plans are in place to mitigate these risks.

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.

Knowledge Services' infrastructure supports multiple data centers within the United States--one in Carmel, Indiana and another in Memphis, Tennessee. Each of the data centers support redundancy, failover capability and the ability to run large scale applications independently in case one center is lost. Our Solution has the ability to guarantee reliability and uptime 99.9% or greater availability. Every component powering the dotStaff™ product is built with minimum N+1 redundancy in the mind, from the power supplies in each server to the data center itself.

- Redundant A / B power feeds backed by battery backup and Diesel generators
- Redundant Multi-Carrier Internet Connections
- Best in class Dell Servers built with redundant power supplies and redundant network connections to our Cisco switch stack
- Redundant Cisco Switches, Cisco ASA Firewalls, Cisco IPS / IDS system and redundant Citrix VPX load balancers
- Redundant data centers: primary data center in Carmel, Indiana and secondary data center in Memphis, Tennessee

Solution Administration (Section 8.16)

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

For our SaaS Cloud Solution, the Purchasing Entity has the ability to add / delete user accounts.

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

Knowledge Services meets the requirement to provide anti-virus protection for data stores.

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

Knowledge Services meets the requirement to migrate all Purchasing Entity data, metadata and usage data to a successor Cloud Hosting solution provider. Knowledge Services will commit to migrating data and to follow any change and communication management strategies the Purchasing Entity may define and / or request.

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

dotStaff™ is a SaaS, multi-tenant Solution. Each tenant's data is protected via our standard product security paradigm. Each client is assigned a Program Manager that is dedicated to the client and supports the Solution as required by the client.

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

dotStaff™ is a SaaS, multi-tenant Solution with varied security models. The Solution hosts a standard security paradigm that drives appropriate password characteristics and reset requirements. The Solution also hosts a high security setting that forces greater password and security complexity and forced reset timetables. The security level is defined by the client and must meet a minimum security setting established by the system which can be increased as required at the time of deployment.

Hosting and Provisioning (Section 8.17)

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

Our Cloud Solution is a SaaS Solution. The Purchasing Entities do not manage or control the underlying infrastructure, such as a network, servers, operating systems or storage.

8.17.2 Provide tool sets at minimum for:

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

Our Cloud Solution is a SaaS Solution. The Purchasing Entities do not manage or control the underlying infrastructure, such as a network, servers, operating systems or storage.

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

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

Knowledge Services' training periods are incorporated in the deployment phase of implementation. We provide training to all stakeholders for clients and vendors / providers during the initiation of the Program and Solution. Knowledge Services will train system administrators and other designated Purchasing Entity personnel on the use of dotStaff™ as it is configured to meet the specific sourcing, billing and administrative processes defined for the State upon completion and approval of future state process maps that will be developed upon award of the contract. Our standard training curriculum includes rules of engagement, on and off boarding procedures, pre-engagement compliance, performance expectations and more.

Testing periods will occur during the deployment and finalization phases of implementation.

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.

Knowledge Services meets the requirement to provide a test and / or proof of concept environment for evaluation that verifies our ability to meet the Purchasing Entity's mandatory requirements through our Desktop Pilot, which is a standard part of our implementation cycle.

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

Knowledge Services will provide training and support for initial implementation and will train system administrators and other designated Purchasing Entity personnel on the use of dotStaff™. Knowledge Services will provide a support team that is accessible 24 x 7 x 365 via online chat, phone support or email. All inquiries are vetted immediately and resolved via our technical support team or, when applicable, escalated to additional support avenues.

Integration and Customization (Section 8.19)

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.

Knowledge Services Solution is commonly integrated to other complementary applications, examples of such integrations include: Project Management Solutions, Procurement Solutions, ERP Solutions, Document Management Solutions, Time Clock Solutions, etc. We have standard API's for the commonly required interfaces and provide a host of interface development options for more complex, less common integrations.

During the implementation discovery meetings with Purchasing Entities, all requested interfaces will be reviewed and standard options explored as a first option.

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

Knowledge Services meets the requirement to configure and personalize the Solutions we provide to meet the needs of specific Purchasing Entities during implementation. During the planning phase of our implementation, we review current state and mapping and recommend future state and workflows based on the information learned from these meetings. The dotStaff™ Solution will be configured based upon approvals from the client.

Marketing Plan (Section 8.20)

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

Knowledge Services would utilize the proven Solution marketing and sales plans, which have resulted in our contract awards with seven State contracts along with dozens of cities, towns and universities through cooperative contracts.

Effective and regular communications are key factors to our success. Solution opportunity education begins early and includes, but is not limited to:

- Promotion at events attended by Knowledge Services such as NASPO Marketing Meeting, NASCIO, and NIGP
- Sales and marketing training and program orientation for the Knowledge Services team
- Webpage creation and marketing on Knowledge Services' website
- Partnership with NASPO ValuePoint to promote via website and other marketing avenues
- State, City and Municipality Informational Seminars
- Targeted outreach and introductions to prospective customers
- Outreach through phone and email communications
- Outreach and presentation to our current vendor / provider partners to spread the word
- Promotion at any State or local events attended by Knowledge Services
- Promotion during one-on-one meetings with interested clients or partners

- Information in blog posts, marketing materials and emails
- Informational sessions for interested clients or partners
- Open house for interested clients or partners with Q&A session

Related Value-Added Services to Cloud Solutions (Section 8.21)

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

The value-added services that Knowledge Services provides as part of and where appropriate an awarded contract for our dotStaff™ Cloud Solution is our Managed Service Provider (MSP) Program service.

> A Managed Service Provider (MSP) is a company that takes on the primary responsibility for managing an organization's contingent and service-based workforce program.

Typically a MSP Program works in conjunction with a Vendor Management System (VMS), such as the dotStaff™ Cloud Solution.

> A Vendor Management System (VMS) is a web-based workforce management Solution providing transparency and governance over the entire workforce (including FTE's) in accordance with the organization's business rules.

The Knowledge Services Cloud Solution automates the contingent labor processes and improves control, transparency and reporting. The Knowledge Services MSP Program service takes the manual process of maintaining a contingent workforce and converts it into a streamlined Solution from initial request for a contingent worker to invoicing. Our MSP program service provides a local and / or dedicated Program Manager, who is available to the client users, providers and vendors in person, via phone and email for support and training.

A MSP Program service adds value in the areas of contingent worker procurement and utilization, reduces the costs associated with contingent engagement and management, minimizes the time spent engaging contingents and ensuring compliance with State's policies and procedures, aligns all job descriptions and increases the overall quality and speed of contingent worker procurement.

Additional Value-Added Services to our Cloud Solution that we can provide as part of an awarded contract include, but are not limited to, consulting services, consulting services pre- and post-implementation, customized training services, customized development services and, where applicable, a complete turn-key solution which may include mobile device hardware.

Supporting Infrastructure (Section 8.22)

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

Knowledge Services requires the Purchasing Entity to have a supported web browser or mobile device to support our Cloud Solution.

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

Infrastructure for Software as a Service are covered by the provider, Knowledge Services / dotStaff™.

Alignment of Cloud Computing Reference Architecture (Section 8.23)

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

Knowledge Services' Cloud Architecture compares to the NIST Cloud Computing Reference Architecture, in particular, the alignment to Software as a Service (SaaS) model, which is accessible from a web browser. The Purchasing Entities do not manage or control the underlying infrastructure, such as a network, servers, operating systems or storage. The essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity and measure service) are transparent to the Purchasing Entities. Broad network access is achieved via a web browser, but provision of computing capabilities, resource pooling, elasticity and measured service is managed by Knowledge Services.

VII. Confidential, Protected or Proprietary Information

All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write "None" in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

Redacted Financial Information.

Confidential

Confidential

VIII. Exceptions and/or Additions to the Standard Terms and Conditions

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations.

If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

Knowledge Services has read and accepts the Master Agreement Terms and Conditions, including the exhibits. We have no exceptions and / or additions to the Terms and Conditions.

None.

knowledge services

Appendix: Technical Proposal

Cloud Solutions

Utah Solicitation No. CH16012
In conjunction with NASPO ValuePoint

Opening Date and Time:

Thursday, March 10, 2016, 1:00 p.m. MTN

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

Appendix

SOC 1 Report

SOC 2 Report

ISP-005 – Data Policy

ISP-006 – Data Policy

dotStaff™ Technology Architecture

March 10, 2016

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

Dear Mr. Hughes,
Knowledge Service is pleased to present our proposal for Cloud Solutions – Utah Solicitation Number CH16012 for the State of Utah, in conjunction with NASPO ValuePoint Cooperative Purchasing Program. Established in 1994 and headquartered in Indianapolis, Indiana, GuideSoft Inc. d/b/a Knowledge Services is a certified Woman-Owned Business Enterprise (WBE) professional services corporation.

Knowledge Services' Cloud Solution will provide the State a proven solution to procure, manage, report and analyze staff augmentation and the mobile workforce. Our Cloud Solution is a proven and repeatable model, providing State governments with predictable, low risk and meaningful results.

The Knowledge Services team members understand and agree that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

The response to this RFP was prepared by the following individuals:

- Joe Bielawski, President
- Dave Stenger, Vice President, dotStaff™ Solution
- Damon Grothe, Vice President
- Cindy Davis, Director
- Emily Kirchmann, Research Associate

Knowledge Services is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

Knowledge Services understands and acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from this RFP.

The service and deployment model that Knowledge Services is capable of providing under the terms of the RFP is Software as a Service (SaaS) and the deployment model is Private Cloud. Our Cloud Solution is capable of storing and securing low and moderate risk data.

On behalf of the entire Knowledge Services team, we appreciate and look forward to the opportunity to work with the State of Utah and NASPO ValuePoint.

Sincerely,

CEO

Julianna Bielawski
CEO
Knowledge Services

KnowledgeServices
Toll Free: 877.256.6948
Office: 317.578.1700
Fax: 317.578.7600
5875 Castle Creek Parkway, Suite 400
Indianapolis, IN 46250
www.KnowledgeServices.com

ATTACHMENT E

Terms of Use

These Terms of Use ("Terms") govern your rights and obligations regarding the use of dotStaff's Software ("Software") and service (both collectively referred to as the "**Service** ") on the Internet or in cellular media. These Terms constitute a fully binding agreement between dotStaff, LLC (including its affiliates and subsidiaries, "dotStaff") the proprietor of all rights in and to the Service, and you. It is therefore recommended that you carefully read these Terms.

By using the dotStaff Service, you signify your assent to

- these Terms;
- dotStaff's privacy policy ("Privacy Policy"); and

If you do not agree to these Terms or any of its parts, then you are prohibited and must refrain from using the Service.

KEY TERMS

The following key points of the Terms are highlighted here for your convenience only. These key points are not made in lieu of the full Terms and their presence in this section does not mean that they are intended to supersede or override any other terms or conditions provided by dotStaff.

Road information prevails. The information provided by the Service is not intended to replace the information provided on the road, such as travel direction, time based restrictions, lane restrictions, road blockades, traffic signs, traffic lights, police instructions, etc.

Cautious driving. Always drive vigilantly according to road conditions and in accordance with traffic laws. It is strictly forbidden to send traffic updates (such as updates on road accidents and traffic congestion), or to non-verbally interact with the Service or use the Service in a non-verbal manner for any purpose other than navigation while driving. Traffic updates or non-verbal reports you want to submit to the Service may only be sent after you have stopped your vehicle in an appropriate location permitted by law. Alternatively, such updates may be sent by a passenger other than the driver, provided it does not interfere with the due course of driving and does not distract the driver's attention to the road.

Emergencies. Always contact 911 in the event of an emergency. Panic button feature availability is not intended as a substitute for contacting 911 or the available authorities in the event of an emergency situation.

Non-continuous updates. The information provided by the Service originates from other users of the Service. Such information is intrinsically fluctuant and may be inaccurate, incomplete or outdated. dotStaff does not provide any warranties to such information's credibility or reliability.

Location-based Service. Some features of the Service make use of detailed location and route information, for example in the form of GPS signals and other information sent by your mobile device on which the dotStaff application is installed and activated. These features cannot be provided without utilizing this technology. Please note, as described in detail in the dotStaff Privacy Policy.

dotStaff uses your location and route information to create a detailed location history of all of your journeys made when using the Service. dotStaff uses this history to offer the Service to you, to improve the quality of the Service it offers to you and to all of its users and to improve the accuracy of its mapping and navigation data. This history is associated with your account and username (if you have chosen to set up a username). This history is retained by dotStaff for a limited period of time and in accordance with the Privacy Policy.

dotStaff allows you to use the Service whether or not you choose to set up a username for yourself. If you choose to use the Service without setting up a username you may do so by skipping the username setup stage of the

application installation process. dotStaff will still link all of your information with your account and a unique identifier generated by dotStaff in accordance with the Privacy Policy.

The Internet connection required to use the Service, and any associated charges (e.g. mobile data expenses) incurred by your use of the Service are your exclusive responsibility and made solely at your expense. Transmitting and receiving real-time updates to and from the Service, requires an online (e.g. Wi-Fi, 3G, 4G) connection between your cellular device and the Internet. The expenses of such connection are as prescribed by the agreement between you and your communication service provider (such as your cellular company) or employer, and according to its applicable terms of payment.

Your age. The Service is intended for use by users who are of the legal age required to hold a driving license.

Privacy. Your privacy is important to us. While using the Service, personal information may be provided by You or collected by dotStaff as detailed in our Privacy Policy found on our website. The Privacy Policy explains our practices pertaining to the use of Your personal information and we ask that You read such Privacy Policy carefully. By accepting these Terms, you hereby acknowledge and agree to the collection, storage and use of your personal information by dotStaff, subject to this section, the Privacy Policy and any applicable laws and regulation.

LICENSE

dotStaff hereby grants you a free of charge, non-exclusive, time-limited, non-transferable, non-sub-licensable, revocable license to use the Service (including the Software) for non-commercial purposes, subject to these Terms.

USING THE SERVICE

You may not: (i) offer to third parties a service of your own that uses the Service; (ii) resell the Service; (iii) offer to rent or lease the Service; or (iv) offer the Service to the public via communication or integrate it within a service of your own, without the prior written consent of dotStaff. For clarity, the examples listed are made for illustrative purposes only; they do not constitute an exhaustive list of restricted activities involving the Service.

You may not copy, print, save or otherwise use data from the Site or the Service's database. This clause does not limit the use of the database as intended by the Software and for the purposes of private and personal use of the Service.

When using the Service or the Site you may not engage in scraping, data mining, harvesting, screen scraping, data aggregating, and indexing. You agree that you will not use any robot, spider, scraper or other automated means to access the Site or the Service’s database for any purpose without the express prior written permission of dotStaff.

The Software may not be used in any way that is not expressly permitted by these Terms.

USE RESTRICTIONS

There are certain types of conduct that are strictly prohibited on the Service. Please read the following restrictions carefully. Your failure to comply with the provisions set forth below may result (at dotStaff's sole discretion) in the termination of your access to the Service and may also expose you to civil and/or criminal liability.

You may not, whether yourself or through any other means or person : (i) copy, modify, adapt, translate, reverse engineer, decompile, or disassemble any portion of the Content included in the Service and/or Site, or in any way or publicly display, perform, or distribute them; (ii) make any use of the Content on any other website or networked computer environment for any purpose, or replicate or copy the Content without dotStaff’s prior written consent; (iii) create a browser or border environment around the Content (e.g. no frames or inline linking); (iv) interfere with or violate any third party or other user's right to privacy or other rights, including copyrights and any other intellectual property rights of others, or harvest or collect personal information about visitors or users of the Service and/or Site without their express consent, including using any

robot, spider, site search or retrieval application, or other manual or automatic device or process to retrieve, index, or data-mine; (v) defame, abuse, harass, stalk, threaten, or otherwise violate the legal rights of others, including others' copyrights, and other intellectual property rights; (vi) transmit or otherwise make available in connection with the Service and/or Site any virus, worm, Trojan Horse, time bomb, web bug, spyware, or any other computer code, file, or program that may or is intended to damage or hijack the operation of any hardware, software, or telecommunications equipment, or any other actually or potentially harmful, disruptive, or invasive code or component; (vii) interfere with or disrupt the operation of the Service and/or Site, or the servers or networks that host the Service and/or Site or make the Service and/or Site available, or disobey any requirements, procedures, policies, or regulations of such servers or networks; (viii) sell, license, or exploit for any commercial purposes any use of or access to the Content and/or the Service and/or Site; (ix) frame or mirror any part of the Service and/or Site without dotStaff's prior express written authorization; (x) create a database by systematically downloading and storing all or any of the Content from the Service and/or Site; (xi) forward any data generated from the Service and/or Site without the prior written consent of dotStaff; (xii) transfer or assign your Service accounts' password, even temporarily, to a third party; (xiii) use the Service and/or Site for any illegal, immoral or unauthorized purpose; (xiv) use the Site, the Service, or the Content for non-personal or commercial purposes without dotStaff's express prior written consent; or (xv) infringe or violate any of these Terms.

TERMINATION OF USE OF THE SERVICE

You may not use the Service after termination of employment. dotStaff retains the right to block your access to the Service and discontinue your use of the Service, at any time and for any reason dotStaff deems appropriate, at its sole and absolute discretion.

USER CONTENT

The Service allows all users of the Software to submit and post information and content to other users ("Content"). Content can include, for example, appointment schedules and updates, notes, map and road updates, traffic congestion updates, road accidents, etc. You assume sole responsibility for any Content you post and you alone are liable for the consequences when you post Content.

ALWAYS DRIVE VIGILANTLY ACCORDING TO ROAD CONDITIONS AND IN ACCORDANCE WITH TRAFFIC LAWS. IT IS STRICTLY FORBIDDEN TO SEND ANY CONTENT - INCLUDING TRAFFIC UPDATES (SUCH AS UPDATES ON ROAD ACCIDENTS AND TRAFFIC CONGESTION) - WHILE DRIVING. YOUR CONTENT SUBMISSIONS MAY ONLY BE SENT AFTER YOU HAVE STOPPED YOUR VEHICLE IN AN APPROPRIATE LOCATION PERMITTED BY LAW.

FORBIDDEN POSTS

It is forbidden to submit Content of a commercial nature (including advertising), unless such posts pertain to dotStaff, the Service, or dotStaff's products, and such Content strictly complies with these Terms.

When you submit Content to be published by the Service, you must make sure it is lawful. For example, you may not submit Content that:

- is diminishing or infringing proprietary rights of others, including but not limited to copyright and trademarks;
- poses a risk to a person's safety, security or health;
- identifies other persons without obtaining such person's express written consent to the disclosure of their personal information, or pertains to minors and identifies minors or their personal information, including their full name, age, address or contact information;
- is unlawful, defamatory, libelous or invades the privacy of others;
- is harassing, offensive, threatening or vulgar;

- is characterized by, or that encourages racism or unlawfully discriminates on the basis of race, origin, ethnicity, nationality, religion, gender, occupation, sexual orientation, illness, physical or mental disability, faith, political view or socio-economical class;
- encourages criminal behavior or conduct that would constitute a criminal offense under any law, or could give rise to civil liability or other lawsuit;
- promotes pyramid schemes, chain letters or disruptive commercial messages or advertisements, or anything else prohibited by law or under these Terms;
- falsely expresses or implies that such content is sponsored or endorsed by dotStaff.

The foregoing examples of unlawful Content are made solely for illustrative purposes and do not constitute an exhaustive list of restricted Content.

COPYRIGHT

All intellectual property rights in and to the Site, the Service and its database, including copyrights, trademarks, industrial designs, patents and trade secrets – are either the exclusive property of dotStaff or its affiliates or are exclusively licensed to dotStaff. The Service is protected, among others, by the United States Copyright Law as well as by applicable copyright provisions prescribed by any other law elsewhere.

"dotStaff", the dotStaff logo, and other trade and/or service marks are the property of dotStaff or its affiliates and you may not use such logos or marks for any purpose that is not expressly authorized in these Terms without the prior written consent of dotStaff.

The design, trade dress, and the 'look and feel' of the maps of the Site and the Service are protected works under applicable copyright laws and dotStaff and its affiliates retain all intellectual property rights in them. The Software license granted to you in these Terms does not extend to or include a license to use the maps displayed on the Software or any mark, indicator, logo or notation embedded in the maps that are displayed on the Software. You may not copy or print more than one copy of any data or material appearing on the Site.

dotStaff may protect the Service by technological means intended to prevent unauthorized use of the Service. You undertake not to circumvent these means. Without derogating from dotStaff's rights under these Terms or under any applicable law, you are advised that any attempted or actual infringement of this provision will result in the termination of all your rights under these Terms. If you circumvent any of the means taken by dotStaff to protect the Service from unauthorized use, you must immediately cease any and all use of the Service, and you undertake to do so.

APPLE

If you use the Service on an Apple device, then you agree and acknowledge that:

Apple, Inc. bears no duties or obligations to you under the Terms, including, but not limited to, any obligation to furnish you with Service maintenance and support;

You will have no claims, and you waive any and all rights and causes of action against Apple with respect to the Service or the Terms, including, but not limited to claims related to maintenance and support, intellectual property infringement, liability, consumer protection, or regulatory or legal conformance;

Apple and Apple's subsidiaries are third party beneficiaries of the Terms. Upon your acceptance of the Terms, Apple will have the right (and will be deemed to have accepted the right) to enforce these Terms against you as a third party beneficiary thereof.

EXPORT CONTROL

You represent and warrant that: (i) you are not located in a country that is subject to a U.S. Government embargo, or that has been designated by the U.S. Government as a “terrorist supporting” country; and (ii) you are not listed on any U.S. Government list of prohibited or restricted parties.

LIMITATION OF LIABILITY AND WARRANTY

DOTSTAFF AND ITS AFFILIATES PROVIDE THE SERVICE AND CONTENT INCLUDED THEREIN FOR USE ON AN "AS IS" AND "AS AVAILABLE" BASIS. THEY CANNOT BE CUSTOMIZED TO FULFILL THE NEEDS OF EACH AND EVERY USER. WE HEREBY DISCLAIM ALL WARRANTIES AND REPRESENTATIONS, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, FEATURES, QUALITY, NON-INFRINGEMENT, TITLE, COMPATIBILITY, PERFORMANCE, SECURITY OR ACCURACY.

Additionally and without derogating from the above clause, dotStaff disclaims any warranties relating to the accuracy of the maps, Content, road conditions, driving directions, navigation routes, or “panic button” functionality presented or displayed in or by the Service. For instance, traffic may be congested in roads depicted by the Service as uncongested; existing roads may be missing from the map; users may submit faulty or inaccurate Content or reports. Such errors and omissions are inherent to any community-based service that operates on users' posts and on the information provided by them.

You agree and acknowledge that you assume full, exclusive and sole responsibility for the use of and reliance on the Service, and you further agree and acknowledge that your use of or reliance on the Service is made entirely at your own risk. You further acknowledge that it is your responsibility to comply with all applicable laws (including traffic laws) while using the Service.

THE INFORMATION PROVIDED BY THE SERVICE IS NOT INTENDED TO REPLACE THE INFORMATION PRESENTED ON THE ROAD. IN THE EVENT THAT THE INFORMATION PRESENTED ON THE ROAD (TRAFFIC LIGHTS, TRAFFIC SIGNS, POLICE, ETC.) INSTRUCTS DIFFERENTLY THAN THE SERVICE, YOU MUST NOT RELY ON THE SERVICE.

dotStaff makes all efforts to provide you with a high quality and satisfactory service. However, We do not warrant that the Service will operate in an uninterrupted or error-free manner, or that it will always be available or free from all harmful components, or that it is safe, secured from unauthorized access to dotStaff's computers, immune from damages, free of malfunctions, bugs or failures, including, but not limited to hardware failures, Software failures and Software communication failures, originating either in dotStaff or any of its providers.

DOTSTAFF, INCLUDING ITS AFFILIATES, OFFICERS, DIRECTORS, SHAREHOLDERS, EMPLOYEES, SUB-CONTRACTORS AND AGENTS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGE, OR ANY OTHER DAMAGE, AND LOSS (INCLUDING LOSS OF PROFIT AND LOSS OF DATA), COSTS, EXPENSES AND PAYMENTS, EITHER IN TORT, CONTRACTUAL, OR IN ANY OTHER FORM OF LIABILITY, ARISING FROM, OR IN CONNECTION WITH THE USE OF, OR THE INABILITY TO USE THE SERVICE, OR FROM ANY FAILURE, ERROR, OR BREAKDOWN IN THE FUNCTION OF THE SERVICE, OR FROM ANY FAULT, OR ERROR MADE BY OUR STAFF OR ANYONE ACTING ON ITS BEHALF, OR FROM YOUR RELIANCE ON THE CONTENT OF THE SERVICE, INCLUDING, WITHOUT LIMITATION, CONTENT ORIGINATING FROM THIRD PARTIES, OR FROM ANY COMMUNICATION WITH THE SERVICE, OR WITH OTHER USERS ON OR THROUGH THE SERVICE, OR FROM ANY DENIAL OR CANCELLATION OF YOUR USER ACCOUNT, OR FROM RETENTION, DELETION, DISCLOSURE AND ANY OTHER USE OR LOSS OF YOUR CONTENT ON THE SERVICE. IN ANY EVENT, YOUR SOLE REMEDY WILL BE LIMITED TO CORRECTING SUCH ERRORS, OR MALFUNCTIONS, AND IN LIGHT OF THE RELEVANT CIRCUMSTANCES.

LOST, STOLEN, DAMAGED DEVICES

User shall be responsible for actual replacement or repair cost for any damage that occurs outside of normal or ordinary wear and tear of the device provided to User. User shall immediately notify dotStaff in the event that a device is lost, stolen or damaged.

LINKS IN THE SOFTWARE

If the Software includes links to services or applications not operated or managed by dotStaff, dotStaff will not be liable for any form of liability arising from your reliance on, or in connection with, the content of such services and applications or any information provided by them, including but not limited to its completeness, accuracy, correctness or it being up-to-date. dotStaff will not be liable for any direct or indirect damage, monetary or otherwise, arising from your use of or your reliance on the content of goods or services you have accessed via links in the Software.

PRIVACY

dotStaff respects your privacy during your use of the Software and the Service. Our updated privacy policy pertaining to the Software is readily accessible at www.dotStaff.com and is an integral part of these Terms. Since the privacy policy is subject to periodic updates, it is recommended that you periodically review the policy for updates.

MODIFICATIONS TO THE SERVICE AND SOFTWARE

dotStaff may, either partially or in its entirety and without being obligated to provide prior notice – modify, adapt or change the Software, the Service's features, the user interface and design, the extent and availability of the contents in the Service and any other aspect related to the Service. You will have no claim, complaint or demand against dotStaff for applying such changes or for failures incidental to such changes.

TERMINATION OF SERVICE

dotStaff may, at any time, terminate the provision of the Service in its entirety or any part thereof, temporarily or permanently, at its sole discretion.

Upon termination of employment, or as otherwise directed by your employer, you will immediately return any mobile device or computers provided to you by your employer for use of the Software and Service.

MODIFICATIONS OF THESE TERMS

dotStaff may modify these Terms from time to time. If fundamental changes are introduced, a notice will be posted in the updated version of the Software as well as on the Service's home page on the Site. Your continued use of the Service after the Terms have been modified signifies your assent to the updated Terms. If you dissent to the updated Terms or to any term within them, you must discontinue all further use of the Software.

GOVERNING LAW AND JURISDICTION

These Terms, the Software and the Service will be governed solely by the laws of the State of Indiana, without giving effect to any conflicts of law principles. Any dispute, claim or controversy arising out of, connected with or relating to these Terms, the Software and the Service, will be under the exclusive jurisdiction of the competent court in Indianapolis, Indiana.

ASSIGNMENT OF RIGHTS

You may not assign or transfer your rights in and to the Service, without the prior written consent of dotStaff. dotStaff may assign its rights in and to the Service to a third party at its sole and absolute discretion, provided that the third party undertakes dotStaff's obligations to you under these Terms.

COMPLETE TERMS

These Terms, together with the policies that are an integral part of these Terms, namely the Privacy Policy and the Copyright Policy, shall all constitute the entire and complete agreement between you and dotStaff concerning the dotStaff Service. In the event of an inconsistency between these Terms and the synopsis of terms presented to the user during Software installation, these Terms shall prevail.

NO LEGAL RELATIONSHIP

These Terms of Use and your use of the Service, including the submission of Content onto the Service, do not, and shall not be construed as creating any relationship, partnership, joint venture, employer-employee, agency, or franchisor-franchisee relationship in any way and of any kind between the parties hereto. Your use of the Service is intended for your enjoyment and benefit and the provision of the Service to you (subject to your compliance with these Terms) constitutes the sole and sufficient consideration that you are entitled to receive for any Content or other contributions you have made to the dotStaff Service, its contents, maps and any other data.

CONTACT US

You may contact us concerning any question about the Service, through the channels listed on the "About" menu in the Software or through the "Contact Us" page on the Site (web address: http://www.dotstaff.com/contact-us/). We will make our best efforts to address your inquiry promptly.

MASTER PRODUCT AND SERVICE AGREEMENT
MOBILE CASE MANAGEMENT SOLUTION

This Master Product and Service Agreement is entered into by and between _____("Client") and GuideSoft, Inc. dba Knowledge Services, including its affiliate, dotStaff, LLC ("Knowledge Services").

1. **Definitions.** The following terms shall have the meaning set forth below:
    a. "Agreement" means this Master Product and Service Agreement.
    b. "Concurrent User" means any User that is logged into the Solution.
    c. "Documentation" means the electronic files and printed materials created by Knowledge Services or its affiliates and made to Client.
    d. "Intellectual Property Rights" shall be defined as any patent, design right, copyright, trademark, service mark (any other application or registration respecting the foregoing), database right, trade secret, know-how and/or other present or future intellectual property right of any type, wherever in the world possible.
    e. "Solution" means the Mobile Case Management Solution provided by Knowledge Services and its affiliates.
    f. "Upgrades" means any future release of the Solution which is made generally available to all of Knowledge Services' end-users. Upgrades are cumulative in that all changes made in previous upgrades are included in the most current upgrade.
    g. "User" means any employee or contractor, consultant, agent or other individual working on the behalf of Client, which Client authorizes to access the Solution.

2. **Grant of License.**
    a. Knowledge Services hereby grants to Client a non-exclusive, revocable, non-transferable and limited license to use the Solution, subject to the terms and conditions in this Agreement and in accordance with the contract term ("Contract Term") defined in the Special Term s and Conditions.
    b. Client's employees and/or contractors ("User(s)") shall sign a User Agreement prior to use of the Solution, which governs the terms of use of the hardware, if provided, and Solution.
    c. Use of the Solution is subject to a Concurrent User limit where a limited number of Concurrent Users may simultaneously be logged into the Solution at any given time. The maximum number of Concurrent Users shall be defined as the total sum of Concurrent Users purchased by Client for any specific term.
    d. Client may, at any time during the Term of this Agreement, increase the Concurrent Limit, as defined in the Mobile Case Management Project Proposal ("Proposal"), by submitting an Order Form to Knowledge Services for such Concurrent Users where Knowledge Services shall apply new fees (and support fees if permitted under any support agreement).

3. **Permitted Uses and Restrictions.**
    a. Client shall be permitted to make such copies of the Documentation to adequately provide to Users and shall not modify, adapt, translate or create derivative works based on the Documentation, in whole or in part, without the prior written consent of Knowledge Services where such work is made publicly available.
    b. Client shall be strictly prohibited from implementing any technology where the effect is to circumvent, directly or indirectly, the Concurrent User limit defined above.

c. Client agrees that if Client makes any modification of the source code, database or any part of the Solution in any way, Knowledge Services is released from any and all obligations.
d. Use of the Solution is for Client's internal purposes and only as permitted pursuant to this Agreement, and shall not be used in any unlawful manner whatsoever.
e. Client shall not assign, sublet or transfer any rights granted herein, except as otherwise provided for in this Agreement.
f. Client shall not rent, lease, transfer, assign, distribute, sell or otherwise provide access to the Solution provided to Client (including through a time-share or through bureau use), in whole or in part, on a temporary or permanent basis, except as otherwise expressly permitted by this Agreement. Client shall not grant any further licenses, sublicenses, or other rights in the Solution. Client will not purport to be an authorized reseller, licensor, distributor, or provider of the Solution to any third party or other organization.
g. Client shall be permitted to make a copy (or copies) of the Solution solely for backup and/ or disaster recovery purposes.

4. **No Implied Transfer of Intellectual Property Rights.** Client and Knowledge Services shall retain ownership of, and all right, title and interest in and to, their respective intellectual property ("Intellectual Property"). No licenses are implied or granted by this Agreement under any patents, licenses, copyrights, trade names, trademarks and any and all other intellectual property rights of Knowledge Services or its affiliates, or other property rights owned or controlled by or licensed to Client. As between the parties, and subject to the terms and conditions of this Agreement, Knowledge Services and its affiliates shall retain ownership of all Intellectual Property Rights in all products or services provided to Client ("Proprietary Technology"). Client acquires no rights to Proprietary Technology except for the licenses or ownership interests granted under this Agreement.

5. **Limitation of Liability**. KNOWLEDGE SERVICES, INCLUDING ITS AFFILIATE, DOTSTAFF, LLC, AND THEIR OFFICERS, DIRECTORS, SHAREHOLDERS, EMPLOYEES, SUBCONTRACTORS AND AGENTS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGE, OR ANY OTHER DAMAGE, AND LOSS (INCLUDING LOSS OF PROFIT, BUSINESS INTERRUPTION AND LOSS OF DATA), COSTS, EXPENSES AND PAYMENTS, EITHER IN TORT, CONTRACTUAL, OR IN ANY OTHER FORM OF LIABILITY, ARISING FROM, OR IN CONNECTION WITH THE USE OF, OR THE INABILITY TO USE THE SOLUTION OR FROM ANY FAILURE, ERROR, OR BREAKDOWN IN THE FUNCTION OF THE SOLUTION, OR FROM ANY FAULT, OR ERROR MADE BY ITS EMPLOYEE, AGENTS, OR ANYONE ACTING ON ITS BEHALF, OR FROM CLIENT'S RELIANCE ON THE CONTENT OF THE SOLUTION, INCLUDING, WITHOUT LIMITATION, CONTENT ORIGINATING FROM INTEGRATIONS WITH THIRD PARTIES, OR FROM ANY COMMUNICATION WITH THE SOLUTION, OR WITH OTHER USERS ON OR THROUGH THE SOLUTION, OR FROM ANY DENIAL OR CANCELLATION OF CLIENT'S USER ACCOUNT, OR FROM RETENTION, DELETION, DISCLOSURE AND ANY OTHER USE OR LOSS OF CLIENT'S CONTENT ON THE SOLUTION. IN ANY EVENT, CLIENT'S SOLE REMEDY WILL BE LIMITED TO CORRECTING SUCH ERRORS, OR MALFUNCTIONS, AND IN LIGHT OF THE RELEVANT CIRCUMSTANCES.

   In the event of any device malfunction, damage or loss, Client shall continue to deliver services as it did prior to this Agreement.

   The Solution may utilize content from third-party applications and providers. Knowledge Services assumes no liability for any damage, injury, loss, or error that may occur as a result of the usage of such third-party applications.

6. **Lost, Stolen, Damaged Devices.** In the event that hardware devices are provided to Client, Client shall be responsible for actual replacement or repair cost for any damage that occurs outside of normal or ordinary wear and tear of the device. Client shall reimburse Knowledge Services for the actual cost of repair in the event that the device is repairable. If the device is lost, stolen or cannot be repaired by Knowledge Services, Client shall reimburse Knowledge Services for its replacement cost, as specified in the Proposal. Client shall immediately notify Knowledge Services in the event that a device is lost, stolen or damaged.

7. **Data Collection.** Data collected by Knowledge Services shall remain the property of the applicable using agency, and such agency must provide express written authorization to Knowledge Services prior to the release of that information to any other agency or third party.

8. **Security and Client Data.** Knowledge Services (including its affiliates) will use commercially reasonable efforts to maintain administrative, physical, and technical safeguards to protect the Client's Data. Safeguards will include, but are not limited to, measures preventing physical or remote access to the server, monitoring of remote access attempts, firewalls and appropriate Solution for the purposes or providing security, all of which are to be made in Knowledge Services' sole discretion. Knowledge Services will use industry standard encryption techniques for any data transmissions by the server.

   The Solution includes certain optional interfaces with third-party applications or use of external communications such as email or SMS that either does not use any encryption or the data encryption is defined by the third-party interface. Use of these features is at sole discretion and risk of the Client.

9. **Data Storage.** Upon written request by the Client, Client may request a copy of Client Data. Upon receipt of such request, Knowledge Services shall provide instructions to the Client on how to receive the Client Data. It is the sole and absolute responsibility of the Client upon receipt of the Client Data to verify that the data is not corrupt, is free of defects and is accessible. The Client is required to notify Knowledge Services of any defects within two (2) days of the Client's receipt of the Client Data. Knowledge Services is under no obligation to notify the Client concerning the return of the Client Data. At any time after fifteen (15) days have passed from the termination date of this Agreement, Knowledge Services is permitted to delete all Client Data in its possession. Client hereby gives its consent for Knowledge Services to delete all Client Data as of the fifteenth (15th) day from the termination date. AT NO POINT WILLL KNOWLEDGE SERVICES RETAIN THE CLIENT DATA BEYOND 15 DAYS FROM THE END OF THE CONTRACT TERM. KNOWLEDGE SERVICES WILL HAVE NO OBLIGATION TO MAINTAIN OR PROVIDE THE CLIENT DATA, AND WILL THEREAFTER DELETE OR DESTROY ALL COPIES OF THE CLIENT DATA IN SERVERS OR OTHERWISE IN KNOWLEDGE SERVICES'S POSSESSION OR CONTROL, UNLESS PROHIBITED BY APPLICABLE LAW.

10. Data Overage. Additional fees may be charged for data used outside of the standard cellular plan.

11. **Support Services.** Knowledge Services will provide support services to the Client during normal business hours. Knowledge Services will, use commercially reasonable efforts to respond to each support request based on the severity of the support request as described below. Knowledge Services does not guarantee any resolution time nor the outcome of any resolution of a support request.

    Each support request will be assigned a severity level by Knowledge Services, in its sole discretion, which determines when the response time is expected. Actual response times may vary.

12. **Termination of Access.** Client shall immediately notify Knowledge Services in the event that any User's access needs to be terminated. Knowledge Services assumes no liability for, including but not limited to, any data breach, improper usage, theft, or damage to any provided hardware device in the event that Client does not notify Knowledge Services of the need to terminate access.
13. **Business Associate Agreement.**

    Client is/is not a covered entity under HIPAA and the terms and conditions of Attachment II "Business Associate Addendum" shall/shall not apply.

14. **Default.** In the event a material breach of this Agreement is not cured within thirty (30) days, after written notice thereof given by the party not in default, in addition to all other rights and remedies either party may have at law or in equity, the non-defaulting party may, at its option, terminate this Agreement as of a date specified in a written notice of termination. In addition, if the material breach involves Client's failure to make required payments under this Agreement, then Knowledge Services may, in its sole discretion, elect to suspend services while Client remains in default rather than terminating this Agreement. In such a case, Client will remain fully responsible for all charges accruing under this Agreement.

15. **Termination.** This Agreement may be terminated by Knowledge Services for any reason, or no reason, by giving Client sixty (60) days' notice. In addition, this Agreement may be terminated at any time by either party, by giving a sixty (60) day written notice of termination or upon the occurrence of any one of the following events:
    (I) Any default by the other party under this Agreement which is not cured within the cure period.
    (II) The cessation of business activities by either party or if the other party is adjudicated as bankrupt or makes a general assignment for the benefit of creditors under any insolvency act, or if a permanent receiver or trustee in bankruptcy is appointed for the property of the party and such adjudication, assignment or appointment is not vacated within sixty (60) days.
    (III) If there is a substantial change in the legal or effective control of either party; a merger, consolidation or reorganization by either party in which either party is not the surviving entity; or the sale, lease or conveyance of substantially all of either party's property, assets or business.

16. **Warranty Exclusion.** KNOWLEDGE SERVICES AND ITS AFFILIATES MAKE NO REPRESENTATION OF IMPLIED OR EXPRESS WARRANTIES OF ANY KIND, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AS APPLICABLE HEREUNDER.

Performance Metric	Goal	Performance Target	Description	Calculation	Frequency of Review/Reporting
dotStaff™ Uptime	99.90%	99.9% or higher	Guarantee of dotStaff availability is greater than 99.9% excluding scheduled dotStaff™ maintenance periods.	365 days per year multiplied by 24 hours = 8,760 hours	Quarterly
Support Response Time	4 Business Hours	92% or higher	Measure average response time from the service request	# of requests responded to within 4 business hours divided by the total number of requests	Quarterly
New User Set Up	8 Business Hours	92% or higher	Amount of time it takes to set up a new user with credentials within dotStaff™	# of new users that are set up within 8 business hours divided by the total number of new users	Quarterly
Increase in field worker efficiency	10% or higher	90% or higher	Improvement in average number of appointments, based upon one hour appointment duration of field workers	The average number of appointment hours or session starts/ends compared to mutually agreed upon historical calculations derived from discovery meetings.	Quarterly
Device Deployment to New User	5 Business Days	92% or higher	Upon confirmed request of new users, amount of time it takes for a new user to receive a fully configured/ provisioned device.	# of new user devices that are provisioned/configured/received divided by the total number of new users	Quarterly
Maintain HIPAA compliance	100%	100%	Must maintain HIPAA compliant methodolgies in all technology and business processes	NIST published guidelines	Quarterly

Performance Metric	MSP/VMS Goal	Performance Target	Description	Calculation	Frequency of Review
Release of staffing opportunities	Staffing opportunities released to all suppliers simultaneously	99%	Measures whether all suppliers have an equal opportunity to supply staff to customers.	Instances of failure to afford equal staffing opportunity.	Annual
Requisition Confirmation Response time	4 business hours	92% or higher	Measures average response time from receipt of request to confirmation of request receipt.	Number of requisitions which received confirmation within 4 business hours / total number of requisitions.	Annual
Resume Submittal Response time	3 business days	92% or higher	Measures average response time from close of proposal to delivery of first candidate's resume.	Number of requisitions which received resumes for review within 3 business days / total number of requisitions.	Annual
Attrition Rate	N/A	10% or lower	Measures resource turnover due to unplanned situations that are	Number of unplanned turnovers / total number of resources.	Annual
Unqualified candidate or Performance Removal	N/A	5% or lower	not caused by the State, not including inadequate performance, death, serious illness, etc.	Number of turnovers / total number of resources.	Annual
VMS uptime	99% uptime	98% uptime	Measures network availability	Contractor's report, monitored by State	Annual
Establish supplier network	Offer suppliers agreements to all existing State suppliers	100% offered	Provides transition opportunity for customers and suppliers	Contractor implementation report(s)	End of Implementation
Monitor supplier network	Annual review of supplier performance	95%	Ensures proper performance of supplier network	Annual report	Annual
VMS security	Preserving security and confidential information present in VMS	100%	Ensures customers, suppliers and employees security is not compromised	Notification of adverse incident & annual report	As needed with annual report
Report submission	Timely submission of reports	98%	Required reports are submitted by specified timeline(s)	Date of report submission	Annual
Customer Service Survey	Bi-annual survey of the satisfaction of the agency requestor with the resource(s) placed at that agency by the contractor. Survey will highlight positive and negative points about the contractor's processes and resources in order to identify areas for improvement. The State Contract Manager will review and include overall results as part of the scorecard.				