



Contract #: AR3088

STATE OF UTAH COOPERATIVE CONTRACT

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

AskReply, Inc. d/b/a B2Gnow

Name

725 West McDowell Road

Street Address

Phoenix

AZ

85007

City

State

Zip

Vendor # VC226559 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact Name: Frank Begalke Phone Number: 602-325-9277 Email: feb@b2gnow.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.
3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.
4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008
5. CONTRACT PERIOD: Effective Date: Monday, April 01, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.
6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.
7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs
- Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.**
9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
 - Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.
10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

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

CONTRACTOR

DIVISION OF PURCHASING

Frank Begalke 4/1/19
Contractor's signature Date

Christopher Hughes
Christopher Hughes (Apr 2, 2019)

Apr 2, 2019

Director, Division of Purchasing

Date

Frank Begalke, COO
Type or Print Name and Title



Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

- (1) A Participating Entity's Participating Addendum¹ ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits² to the Master Agreement;
- (3) The Solicitation;
- (4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
- (5) A Service Level Agreement issued against the Participating Addendum.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

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

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

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

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

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

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

10. Defaults and Remedies

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

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

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

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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

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

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

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

13. Indemnification

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

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

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

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

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

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

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

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and

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

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

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

16. Insurance

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

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

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

aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

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

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

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

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

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

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

a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

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

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

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

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

19. Ordering

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

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

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

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

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

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

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

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

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

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

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this

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

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

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office³.

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

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

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

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate

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

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

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

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

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

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

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

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

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

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

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

26. Records Administration and Audit.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Services it acquires from this Master Agreement.

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

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

32. Transition Assistance:

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

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

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

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

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

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

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

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

37. Governing Law and Venue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

within the Participating State.

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

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

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

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

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

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Service (SaaS)

1.2 Risk Categorization.*

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

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	B2Gnow	B2Gnow		Community

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

2.1 Deployment Models.

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

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

Attachment C - Pricing Discounts and Schedule

Contractor: AskReply, Inc. d/b/a B2Gnow

Pricing Notes

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

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
SaaS Minimum Discount % *	
(applies to all OEM's offered within this SaaS model)	15.00%
Average SaaS OEM Discount Off	15.00%

<u>Item Description</u>	<u>Onsite Hourly Rate</u>		<u>Remote Hourly Rate</u>	
	<u>NVP Price</u>	<u>Catalog Price</u>	<u>NVP Price</u>	<u>Catalog Price</u>
Maintenance Services	N/A	N/A	N/A	N/A
Professional Services				
Deployment Services	N/A	N/A	N/A	N/A
Integration Services)	N/A	N/A	\$ 153.00	\$ 180.00
Consulting/Advisory Services	N/A	N/A	\$ 306.50	\$ 360.00
Architectural Design Services	N/A	N/A	N/A	N/A
Statement of Work Services	N/A	N/A	N/A	N/A
Partner Services	N/A	N/A	N/A	N/A
Training Deployment Services	N/A	N/A	N/A	N/A
Data Entry Services			\$ 76.50	\$ 90.00
Data Integration Services			\$ 153.00	\$ 180.00
Custom Reporting Services			\$ 153.00	\$ 180.00
Custom Enhancement Services			\$ 153.00	\$ 180.00
Supplemental Training Services			\$ 153.00	\$ 180.00
Supplemental Project Management Services			\$ 153.00	\$ 180.00
Program consultation and process analysis			\$ 306.50	\$ 360.00

Deliverable Rates

	<u>NVP Price</u>	<u>Catalog Price</u>
	N/A	N/A

TECHNICAL RESPONSE

Robust, flexible B2Gnow Diversity and Vendor Management software, coupled with our proven implementation services, delivers a solution that will meet the Purchasing Entities' requirements out-of-the-box.

Our proposed service is the B2Gnow Diversity and Vendor Management System in a hosted SaaS environment. Implemented by B2Gnow, the solution will provide an enterprise-wide diversity and vendor management system. The proposed system meets all technical requirements outlined in the RFP. Although B2Gnow is an out-of-the-box solution designed specifically for government compliance needs, it is highly configurable to meet the unique needs of each Purchasing Entity without time-consuming and expensive customization.

The B2Gnow system is modular with over twenty available modules that can be implemented in any combination to meet the needs of each Purchasing Entity.

SYSTEM ACCESS FOR USERS IS 24/7

B2Gnow is a 100% web-based system with guaranteed availability of at least 99.9%. As a result, the system is available 24/7 from anywhere with Internet access. Use of the B2Gnow system does not require any downloads, plug-ins, or cookies for either agency staff or its contractors/vendors to access.

DATA OWNERSHIP AND RETENTION

The Purchasing Entities retain complete ownership rights to all data added to the system by their staff or vendors whether through manual entry or data interfaces. B2Gnow maintains no rights to the Purchasing Entities' data and will only disclose or release data upon explicit instruction from approved staff.

The Purchasing Entities' data will remain in the system for the duration of our engagement or until B2Gnow is instructed to archive or delete historic data. B2Gnow will comply with any data retention, deletion, or archive requirements that the Purchasing Entities are subject to. The Purchasing Entities can export their data from the B2Gnow system at anytime without assistance from B2Gnow staff. Furthermore, at the end of our engagement B2Gnow will provide the Purchasing Entities with a complete electronic copy of all its system data.

All Purchasing Entities' data (primary and backup) will remain, at all times during transmission and storage, within the continental United States. All access points to data shall be from within the continental United States.

HOSTING, SYSTEM BACK-UP AND DISASTER RECOVERY

As a hosted SaaS solution B2Gnow guarantees availability of 99.9%. We have always exceeded this guarantee and typically operate above 99.99%. B2Gnow maintains redundancy at every level of our architecture. We utilize multiple co-location facilities (each with redundant power, HVAC, & bandwidth), load balancers, redundant servers & devices at each node, database mirroring, and disk-disk-tape backup.

B2Gnow utilizes 3rd-party services to monitor system availability from multiple locations around the country every sixty seconds. If the system experiences an outage, B2Gnow system administrators and senior management are notified immediately.

B2Gnow's backup procedure has been designed to guarantee that no more than 4 hours of data would be lost due to a complete system failure, which has never occurred in the system's history. If a primary database server should fail, the system will automatically direct traffic to the redundant server. If both servers fail, the production database is backed up on disk to a separate server every four hours. Additionally, backups are archived to a separate environment weekly.

In the case of catastrophic system failure, we maintain a full disaster recovery environment available for rapid switchover and at least three additional training, testing, and development environments with full functionality that could be utilized at any time. The transition plan is executed quarterly to ensure all elements are operational. The Purchasing Entities' system will be covered by this plan.

We have also included a B2Gnow Technology & Security Overview document in Appendix A for your review and welcome any additional technical questions you may have.

SECURITY CAPABILITIES

B2Gnow has implemented industry-standards for security access control including user specific logins, complex passwords, password expiration, concurrent logins (not permitted), and the ability to restrict or permit access based on IP range.

B2Gnow protects against unauthorized data access on several levels. Each individual accessing the system is required to have a unique login and password. The system enforces complex password requirements and does not permit concurrent logins. The system incorporates a triple-tier firewall architecture and is monitored 24/7, both internally and by 3rd-party firms, for intrusion detection and unauthorized access.

B2Gnow has never experienced unauthorized access to the system or data during our entire history.

SYSTEM MONITORING

B2Gnow utilizes three 3rd-party services (24x7, Alertra, & Pingdom) to monitor system availability and performance from cities across the country. In addition to immediately alerting our staff to system issues, these services track B2Gnow system availability.

REPORTING ENVIRONMENT OVERVIEW

B2Gnow includes over 400 standard reports that have been designed in collaboration with our customers. Standard reports are included for all modules. Most standard reports can be run in several formats – to screen, PDF, Excel, Word, and CSV.

B2Gnow vendor and contract search functions allow for powerful data extracts. Users can perform a search using relevant field selection and while reviewing the search results they can choose to "Export". This allows the user to select what fields they want to export and then export the search results to CSV/Excel.

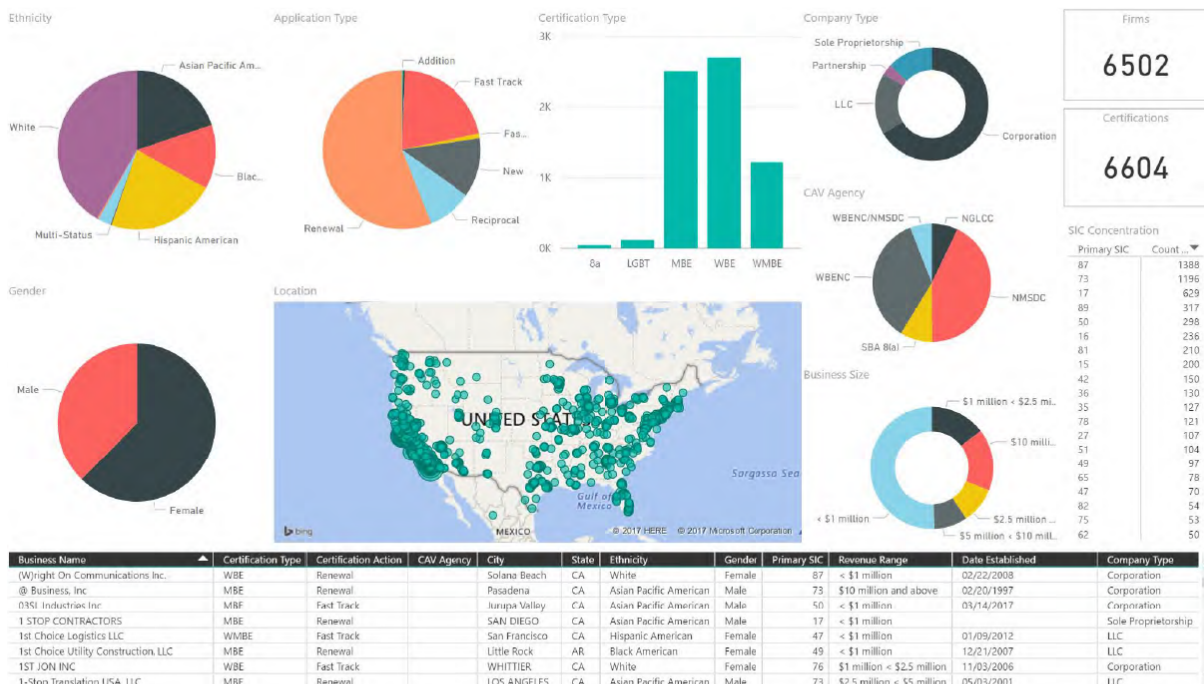
B2Gnow also provides staff users with true Ad Hoc reporting using Microsoft Reporting Services. This powerful tool allows Purchasing Entity staff to create their own reports and save them for future use. B2Gnow offers training and support on the ad hoc tool to assist Purchasing Entity staff in

State of Utah / NASPO ValuePoint SK18008 – Master Agreement for Cloud Solutions



learning to use the tool. B2Gnow is in the process of rolling our Power BI as a new, easier to use and more powerful ad-hoc tool.

Lastly, custom reports can be designed and produced for a unique reporting need or derived from an existing standard report with Entity-specific modifications. Report requirements are assessed and a proposal provided by B2Gnow that encompasses the time and materials to deliver the report.



SYSTEM INSTALLATION AND UPDATES

B2Gnow is provided as a hosted SaaS solution and, unlike traditional software, does not require installation. The system is currently being used by customers all over the United States. Adding a new client, like a NASPO Purchasing Entity, involves creating a new account within the system and configuring the account to meet the client's needs. This allows us to provide new clients with initial system access in only a few days.

B2Gnow also manages all system updates in a manner that is transparent to the users. Our technical architecture allows B2Gnow system administrators to apply system upgrades with no system downtime.

TEST ENVIRONMENT

B2Gnow will provide the Purchasing Entities with access to a test environment. The test environment will be available throughout the entire length of our engagement. The test environment will be a replica of production, and will allow staff to test, validate and train in a non-production environment.

During the implementation, B2Gnow will configure each module based on each Purchasing Entities requirements. Your staff will then have the ability to test the configuration and validate that the

system meets the requirements. This detailed validation process will guarantee that the go-live of the B2Gnow system will not be disruptive to the existing systems and processes.

PURCHASING ENTITY IT REQUIREMENTS

As a hosted SaaS solution, IT requirements for the Purchasing Entities are minimal. To access the system, users need only a PC with Internet access. The system does not require any plug-ins or 3rd-party software for user access.

Because B2Gnow is a hosted solution, there is no hardware or software for the Purchasing Entities to purchase, install, or maintain. B2Gnow system administrators will manage the entire technology infrastructure.

B2Gnow will work with your IT team during any initial data conversion and to create any interfaces between B2Gnow and existing Purchasing Entity systems. Typically, these are defined tasks of the overall project plan and only require IT interaction on a limited basis for a four week period.

TECHNICAL PLATFORM

B2Gnow is a proven SaaS solution with thousands of daily staff and vendor user logins. Our technical infrastructure has been in place since 2001 and is upgraded continually to meet the needs of our expanding customer base. Included in Appendix A is a technology and security overview that details all parts of our infrastructure. We maintain dual or better redundancy at every level of our infrastructure (facility, power, connectivity, firewalls, load balancers, switches, servers, databases, etc.) and adhere to industry best practices. B2Gnow has always exceeded 99.9% availability and has never experienced any loss or breach of data.

B2Gnow's system team continually monitors and assesses system use, performance, and availability. Server capacity (power, memory, storage) is increased to ensure a substantial margin between need and capacity. With over 500,000 users, the system is sized to handle thousands of concurrent users and provide response times below one second for the vast majority of system actions. Hosted on the Amazon AWS platform, the access bandwidth is substantial, which supports high volume and large size file uploads and downloads. The system currently supports online reporting by other very large organizations, including New York, Illinois, Washington, and Tennessee with no performance degradation.

SOFTWARE MAINTENANCE AND SUPPORT

B2Gnow will perform all software and system maintenance activities as part of the scope of services for this contract. Such activities include, but are not limited to, server management, software patches, software upgrades, software fixes, system enhancements, system releases, deployment and configuration of the latest features, performance improvements, and other activities related to assuring the availability and performance of the system. All standard enhancements and upgrades related to the functionality deployed and configured for the Purchasing Entities' systems will be provided as part of the annual service fee.

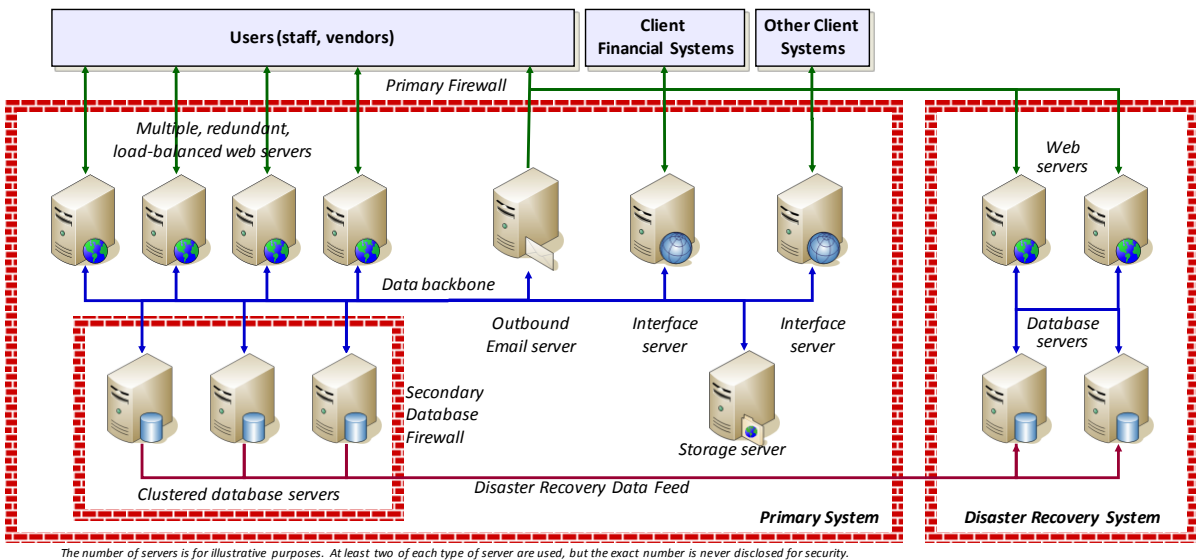
SYSTEM ARCHITECTURE

B2Gnow manages millions of records while being secure, robust and scalable. Web servers are load-balanced and exchange data with a set of clustered database servers. Important data is stored on a redundant disk array that is regularly backed up. Inbound and outbound data is processed by a set of

interface servers that perform all required actions and either save the information to the database, or send it on to the designated customer system.

As a multi-tenant architecture, B2Gnow is a shared system which was built with adequate security to ensure that an agencies data can not be accessed by any other party. B2Gnow has never had a situation where system data has been lost or compromised in any way.

Below is a diagram detailing the system architecture:



INTERFACES

B2Gnow has extensive implementation and integration experience with enterprise-level financial, procurement and data warehouse systems. B2Gnow has successfully interfaced with over 100 external systems during customer implementations.

Interface development is based upon the B2Gnow Data Implementation Process, and is well-documented and tested through dozens of projects. The most efficient method for data exchange is for the information to be provided as a flat file on a secure SFTP server account. Data will be considered verified and ready for export when placed on the SFTP server. All data manipulation, filtering and verification will be performed before being placed on the SFTP server.

HISTORIC DATA MIGRATION

B2Gnow uses an established methodology for migrating historic data to the system. Data templates for selected record types (e.g. vendors, contracts, payments, etc.) guide each Purchasing Entity to identify relevant information, standardize the input, and streamline the process. The final data sets are then loaded into the configured system by B2Gnow. Data that is not ready-to-load, unduplicated, clean, well-defined, and in an approved electronic format may require additional work outside of the project scope.

PROCESS ANALYSIS AND INCORPORATION

A significant part of the value B2Gnow's team can bring to each Purchasing Entity is the experience we have amassed through dozens of successful implementations. Our standard project plan includes a

review of each Purchasing Entities' current compliance processes. During this stage, B2Gnow will suggest process improvements based upon best practices we have witnessed at other organizations. Upon approval by the agency, the B2Gnow implementation team will configure the system to support any revised processes. The B2Gnow system is highly configurable and can easily accommodate each Purchasing Entities' specific process needs, especially as they change in the future due to the regulatory and policy environment.

TRAINING AND ONGOING SUPPORT

B2Gnow's training team will develop a comprehensive training plan that meets all each of the Purchasing Entities' requirements. As an existing SaaS solution, B2Gnow will leverage our experience training dozens of other large organizations to create an effective training plan. The training plan will be presented to the agency for approval before implementation.

B2Gnow staff maintains extensive training materials that have been used in training thousands of users.

Initial training will be performed onsite for staff with training sessions broken into key functional areas (i.e. contract compliance, bid tracking, etc.). Training will be instructor-led, using "real-life" data and scenarios, and supplemented with complete user manuals and quick guides. All of staff "trainers" can participate in the initial onsite training sessions.

In addition, B2Gnow offers ongoing web-based refresher training and training for new staff members throughout the contract term at no additional fee. Refresher training can be accomplished through our regularly scheduled training webinars, or by arranging one-on-one sessions through support. Onsite follow-up training is also available, but is billable.

Vendors typically require very little, if any, training due to the intuitive nature of the process and detailed online documentation. We can incorporate initial vendor training as part of the on-site or web-based training sessions during implementation. Vendors may also sign-up for regularly scheduled vendor training webinars.

SUPPORT SERVICES

As a hosted solution, your annual service fee is comprehensive. In addition to guaranteed system access, availability and software updates, B2Gnow provides unlimited technical problem-solving support. Support is provided by phone, email and online to staff. For vendors, support is provided by email with a maximum 48 hour response time. Issues, questions and concerns from vendors regarding transactions and other account updates will be directed to the designated agency staff member.

TYPES OF SUPPORT

B2Gnow offers comprehensive customer support services to meet our customers' needs. B2Gnow's standard support package includes:

- Product updates
- Telephone support
- Online support through email and the Internet
- User training webinars
- User manuals and quick-guides

The primary method of contacting Customer Support is through the system. The B2Gnow system has a built in support capture mechanism that collects relevant information and routes it immediately to the support team, resulting in the fastest response. An integrated Help Desk module identifies the user to support staff and permits the first available team member to review and respond to the query.

Users can ask any type of question, and queries regarding each Purchasing Entities' program received by B2Gnow Customer Support will be assigned to the appropriate staff member. Staff users are able to use the Help Desk module to respond to queries, which then maintains a history of all support contact.

A dedicated email address will be configured to collect and log email support queries into the Help Desk module. Once recorded, they are viewed and answered in the same manner.

Purchasing Entities staff can contact support by telephone for priority issues. Vendors are encouraged to contact support through the system or email for fastest response, but B2Gnow support staff are authorized to respond to vendors by phone if necessary to resolve an issue.

B2Gnow offers regular training webinars to all staff and vendor users. Users can register for a class and attend while sitting at their computer. User manuals and quick-guides are provided in PDF format for download and short instructional videos are available to guide users in the completion of system actions.

LEVELS OF TECHNICAL SUPPORT

All users of B2Gnow are provided with the high quality technical support. There are three tiers of support provided based on user type, user experience, and nature of the issue.

- Tier 1: account access and management issues; standard system use
- Tier 2: experienced staff users; advanced system use
- Tier 3: complex situation; most complex system use

Tier 1 support is typically provided to all vendors and newer staff users. Experienced staff may opt-in for automated escalation to the Tier 2 support team. Tier 3 support handles escalations from Tiers 1 and 2. Within each support tier, staff respond to support tickets in the order in which they are received. Support tickets may get escalated to staff if the support topic is beyond technical support.

HOURS OF AVAILABILITY

B2Gnow's support departments are available during the hours listed below. Times are for standard support; additional hours of support are available on a negotiated case-by-case basis.

Customer Support: 8:00 am EST to 6:00 pm PST Monday through Friday

Technical Support: 8:00 am EST to 6:00 pm PST Monday through Friday

Each Purchasing Entity will be provided with after-hours contact information for emergency situations.

RESPONSE TIMES & ESCALATION PROTOCOL

Response times for customer and technical support requests are detailed in the B2Gnow Service Level Agreement. This document includes a documented escalation protocol for resolving reporting issues. Please refer to Appendix A for details.

PRIORITY & SEVERITY LEVELS

B2Gnow will diligently work for the prompt resolution of defects and errors in the software, hardware, or connectivity of the B2Gnow Service. System problems can be submitted by phone, email, or internally within the system.

The customer is best able to assign a severity level to a problem; however, B2Gnow Technical Support will ask questions to assure the right resources are assigned. When reporting a problem or updating the status of an incident, customers should always call B2Gnow's main support number rather than a particular B2Gnow employee. If a Severity 1 or 2 problem is encountered with the system (e.g. system failure or unavailability), inform the first representative when placing the call in so the problem is be escalated to the correct person as quickly as possible.

B2Gnow will respond to and complete correction of errors, defects and malfunctions, in accordance with its defined issue resolution policy.

Errors within the system are automatically logged with an email alert sent to the B2Gnow support team. Typically, the support team is aware of an issue before users report it. Team members will proactively monitor the system to analyze user behavior and system response.

DOCUMENTATION

User documentation for users will be provided in multiple formats, including onscreen content, an online help system, and printable user manuals and quick guides. The content in the documentation is updated regularly and is available to each Purchasing Entity for its own publication. Additionally, online video help is available for both staff and vendors.

IMPLEMENTATION OVERVIEW

B2Gnow has a long track record of successfully implementing diversity and vendor management systems with large governments. This experience will be leveraged for each Purchasing Entity project to ensure a project that is finished on time with the committed functionality.

IMPLEMENTATION METHODOLOGY

B2Gnow is a proven, turn-key SaaS system that allows for quick implementation and start-up. Being a hosted solution, there is no hardware to be purchased or software to be installed by each Purchasing Entity. The system is highly configurable to meet each Entity's specific program needs without the need for customization. As a result, the implementation can be completed in weeks, not months.

Over the course of more than 200 successful implementations, B2Gnow has developed and refined a standard implementation methodology. The project will be assigned an experienced project manager who will guide each Entity through the implementation process. Highlights of our implementation process include:

- **Kick-off Meeting:** Review scope; establish project plan, timeline and resource list
- **Weekly Project Calls:** To review status and manage the schedule
- **Portal Creation:** The Entity will participate in a portal configuration exercise that results in a custom system portal that matches the desired look and feel
- **Module Configuration:** Each module has a detailed document that outlines all configuration options and decisions needed. Established configuration guides facilitate faster, more accurate implementations
- **Notification Templates:** The Entity will review and edit a detailed notification template for B2Gnow to customize system-generated email and letter formats
- **Data Migration:** Utilize standard data migration formats that highlight required and optional fields; standard formats allow easy and accurate data migration
- **Integration:** Follow B2Gnow's established integration guide and data layouts to expedite the process; our technical team will manage the integration process
- **Training:** B2Gnow has standard training courses for each module; training will be customized for Entity-specific processes and requirements
- **Go-Live:** Detailed checklists utilized to prepare both client and its contractors for a successful "go-live"
- **Project Oversight:** B2Gnow's executive management team provides regular project oversight to guarantee client satisfaction, and is continually accessible throughout the entire contract term

While B2Gnow has developed a standard implementation process with detailed templates and guides, we realize that every customer is unique. The tools we have developed provide a proven methodology, while allowing the project manager to tailor the implementation tools to meet the Purchasing Entity's specific needs. This approach allows for a best-of-both-worlds implementation approach.

SOFTWARE FAMILIARIZATION SESSIONS

A familiarization session will be provided to Entity staff and anyone closely familiar with relevant internal and external processes so they can visualize how system functionality will meet their needs. The sessions are intended for any staff that will be involved in the project and the goal is to initiate staff consideration of how their procedures will translate to the new system.

PROCESS ANALYSIS AND INCORPORATION

A significant part of the value B2Gnow's team can bring to each Entity is the experience we have amassed through the dozens of successful implementations. Our standard project plan includes a review of the organization's current processes. During this stage B2Gnow will suggest process improvements based upon best practices we have witnessed at other organizations. Upon approval by the Entity, the B2Gnow implementation team will configure the system to support any revised processes. The B2Gnow system is highly configurable and can easily accommodate the organization's specific process needs, especially as they change in the future due to the regulatory and policy environment.

STREAMLINED IMPLEMENTATION

B2Gnow is a proven, turn-key system that allows for quick implementation and start-up. Being a hosted solution, there is no hardware to be purchased or software to be installed by the Purchasing Entity. The system is highly configurable to meet each Entity's specific program needs with standard configuration.

SYSTEM CONFIGURATION

PUBLIC WEB PORTAL

The portal provides for the viewing of all public information, such as supplier onboarding steps, account lookup and password reset functions, and posting of relevant public records. All features are optional and the structure of the portal will be configured in a manner that meets the Purchasing Entity's requirements for information disclosure.

B2Gnow will configure the "front end" of the system to best represent the Purchasing Entity's web page. The web address of the portal will be selected from domains under B2Gnow's control, such as suppliercompliance.us or vendorreg.com, and will be preceded by a label of the Purchasing Entity's choosing, such as "Utah", for example <https://utah.diversitycompliance.com/>.

The Purchasing Entity can link to the system from any of its web sites. Configuration of the public web portal includes setup of standard notification templates, including user account management configuration, online application notices, registration notices, training notices, and other standard alerts that are part of the baseline system and designated modules.

MODULE CONFIGURATION

The configuration of each B2Gnow module involves the selection of several options on one or more user interface web pages. The settings will be reviewed with the Purchasing Entity, and B2Gnow staff will update each setting to best support the organization's program. Some modules contain a half dozen settings, others contain over one hundred. After the initiation module configuration, and each update afterwards, a copy of the configuration is taken in PDF format for reference purposes.

STANDARD REPORTS

Each B2Gnow module includes dozens of standard reports. From simple lists of vendors and certifications to sophisticated analytics, the standard reports provide the Purchasing Entity with dozens of options to analyze and view its data. Reports can be exported to Excel, Word, and PDF format.

AD-HOC REPORTING

B2Gnow's baseline system includes many "data models" that represent data in the system. Data models compile database records into easy-to-use blocks that do not require advanced programming skills to access. Field names are in plain language and record types connected in logical formats.

Based on the final configuration of the system, B2Gnow will design, create, and publish additional data models to support ad-hoc access to data in the Purchasing Entity's system.

PROJECT SCHEDULE

A typical project is detailed below in a sample implementation schedule which reflects B2Gnow's rapid implementation process while ensuring maximum quality and minimizing project risk. Project schedules range from two to nine months from kick-off to go-live, depending on the number of modules, data interfaces, and migration included in the scope of work.

Based on experience with similar projects, the schedule chart below shows a recommended sequence of implementation for the modules; this will be reviewed and adjusted as needed at the start of the project. Upon project initiation, a daily/weekly schedule is developed in conjunction with each Entity's project management staff.

Our team places great importance on achieving the set schedule goals of this initiative, and on ensuring that expectations are reasonable and attainable. With close cooperation between each Purchasing Entity and B2Gnow, it is possible to have the system launched within weeks, and at full utilization within months. Our team is confident of achieving the target schedule dates with the support of each Entity.

The proposed schedule assumes that all information is ready at the beginning of the project. Any cleaning or updating of the information may require more time.

Task	Week																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Notice to Proceed	█																
Project Kick-Off		█															
Vendor Management Module Configuration			█	█	█	█											
System Portal Configuration				█	█	█	█										
Contract Compliance Module Configuration					█	█	█	█									
Online Application Module Configuration						█	█	█	█								
Certification Management Module Configuration							█	█	█	█							
Labor Compliance/Prevailing Wage Module Configuration								█	█	█	█						
Outreach & Event Management Module Configuration									█	█	█	█					
Report Configuration										█	█	█	█				
Third-Party System Integration											█	█	█	█			
Migrate Existing Data												█	█	█	█		
Training														█	█	█	
Go-Live																	█

PROJECT MEETINGS & REPORTS

PRE-PROJECT MEETINGS

One or more conference calls with the Entity's project team will be conducted to make introductions, review the scope of work, discuss and refine functional requirements, review the initial project calendar, and set expectations for the onsite kick-off.

PROJECT KICKOFF

To officially commence the project, a meeting of the B2Gnow and the Purchasing Entity's project managers and key staff will be held. The purpose of the meeting will be to finalize the project schedule, reaffirm the deliverables, review roles and responsibilities, and discuss relevant project processes, including a schedule for weekly status meetings and any other necessary near term meetings. The date of the kickoff meeting shall be the official start date of the implementation.

PROJECT STATUS MEETINGS

B2Gnow's project manager will coordinate weekly project status meetings on a set day and time. Status meetings will include the project managers, key project team members, and Executive Management from B2Gnow and the Purchasing Entity. Weekly status meetings will be conducted either by conference call or in person.

Other project meetings will be scheduled in advance with all required personnel. Every effort will be made to schedule meetings as far in advance as possible. It is assumed that all required resources will have sufficient availability for the duration of the projects. Limitations on resource availability or cancellation of meetings will have a negative impact on the overall project schedule.

PROJECT NOTIFICATIONS

Notices, requests, announcements, reports, and other communications regarding this project are considered delivered when sent via email, fax, or mail, and are not bounced, failed, or returned. Voicemail is not considered a valid medium for official project correspondence.

PROJECT STATUS REPORTS

B2Gnow will provide weekly project status reports. Tasks assigned to the Purchasing Entity will also be included to ensure that staff are knowledgeable about the schedule and data requirements of the project.

Status reports include:

Project Status: Overall project status indicator (green, yellow, red)

Target dates (both past and future): All key project dates and status of each

Main activities: Major accomplishments and events of the past week and planned activities in coming week

Issues: Any problems that required immediate resolution to keep the project on schedule

Activities by milestone: A review of each major milestone and the accomplished sub-steps for each

System statistics: Summary and detailed statistics of the system's operation, including audits, responses, registrations, accounts, contracts and certifications

PROJECT MANAGEMENT TOOLS

Over the course of more than 200 implementations, B2Gnow has developed and refined a proprietary set of implementation tools, templates and documents. These tools will be used throughout the implementation process to guarantee project success.

B2Gnow's implementation library includes:

- Project implementation plan template
- Project status update template
- Portal configuration guide
- System notification templates
- Module configuration guide (for each module)
- Data migration guide & data migration file layout template
- Data interface guide & data interface file layout template
- Training plan
- Sample system announcements
- Internal and public go-live checklists
- Post go-live checklist

TECHNICAL REQUIREMENTS

The following pages contain B2Gnow's point by point response to each technical requirement. B2Gnow only offers a SaaS solution.

#	Requirement	B2Gnow Response
8.1 TECHNICAL REQUIREMENTS		
8.1.1	For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145 .	The B2Gnow solution meets all five essential characteristics of NIST SP800-145: 1. On-demand self-service: Clients have 24/7 access to the B2Gnow system. The system automatically allocates additional resources as needed. 2. Broad network access: The B2Gnow system can be accessed from any device with Internet access. 3. Resource pooling: B2Gnow is a multi-tenant architecture with pooled computing resources located in the US. 4. Rapid elasticity: The system is load-balanced and provisioned dynamically to respond to client computing needs. 5. Measured service: Resource usage can be limited based on capacity needs of each client.
8.1.2	As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D .	Yes; As applicable to our offer, B2Gnow will comply with Attachment C – NIST Service Models and Attachment D – Scope of Services.
8.1.3	As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D .	Based on the included definition, B2Gnow is a cloud based service provider. Based on the typical data managed in our system, our categorization of risk would be Low Risk Data. B2Gnow meets all five essential characteristics of the NIST SP800-145 cloud based service model (see 8.1.1). B2Gnow meets the NIST definition for the service model of Software-as-a-Service (SaaS). B2Gnow is provided to clients as an application running on a cloud infrastructure available via a web browser. As a multi-tenant architecture, B2Gnow meets the definition of a Community cloud deployment model.

#	Requirement	B2Gnow Response
8.2 SUBCONTRACTORS		
8.2.1	Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that 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.	B2Gnow intends to provide our cloud solution and all services directly without the need for 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.	B2Gnow does not intend to utilize 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.	Not applicable.
8.3 WORKING WITH PURCHASING ENTITIES		
8.3.1	Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as: Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;	On a semi-annual basis B2Gnow communicates to all clients its protocols for preventing, detecting, and resolving a breach. B2Gnow's Security Officer is responsible for preventing, and in the event of a breach managing the communication and remediation of the breach. B2Gnow's Security Officer, Chief Operating Officer/Contract Manager, and Chief Executive Officer/System Architect would all be involved at all stages of a data breach.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
	• Response times; • Processes and timelines; • Methods of communication and assistance; and • Other information vital to understanding the service you provide.	In the event of a data breach, clients would be notified within a maximum of 48 hours. Once a data breach is detected the system will be taken offline immediately to prevent further data loss. The security breach will be evaluated and remediated before the system is brought back online. B2Gnow will evaluate the extent of any data breach or loss and provide this information to each client. B2Gnow will work with all affected clients to manage the data breach. Initial communication would be via email and the system portal page. B2Gnow contract manager/COO would follow-up directly via phone to all purchasing entities. B2Gnow takes data security seriously. Over B2Gnow's nineteen-year history no data has been lost or compromised in anyway.
8.3.2	Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.	The B2Gnow system does not allow adware, unauthorized software, or any type of marketing to be generated or sent via the platform.
8.3.3	Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.	Yes; B2Gnow provides clients with access to a test/staging environment that is identical to production. Clients have access to the test/staging environment for their entire engagement with B2Gnow.
8.3.4	Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities, and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.	Yes; B2Gnow maintains ADA 508 accessibility compliance. B2Gnow can provide a 508 Voluntary Product Accessibility Template (VPAT) upon request.
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 a minimum.	Yes; The B2Gnow system and all content is delivered via web browser. B2Gnow supports the current version of all listed browsers plus at least three previous versions.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
8.3.6	Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.	As part of our standard client onboarding B2Gnow staff will meet with the Purchasing Entity to finalize a Statement of Work and Service Level Agreement. Part of this discussion includes review of sensitive or personal data and the specific law, rule, or regulations that must be complied with.
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.	B2Gnow has developed and refined a standard implementation methodology to guarantee client success. An overview of this project plan has been included in the Implementation Overview section of this proposal (page 10).
8.3.8	The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe: • How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein. • How Offeror will maintain discounts at the levels set forth in the contract. • How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates. • How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.	As a SaaS solution B2Gnow is continually releasing new enhancements to stay current with technological changes, client functional needs, and regulatory changes. All enhancements and updates will be done in compliance with all requirements of this RFP. B2Gnow will continue to offer the same minimum discount throughout the life of this contract. B2Gnow publishes release notes on the system portal page for all clients to see. Major updates will be communicated via email to all Purchasing Entities in advance of their release date. B2Gnow is typically able to deploy new enhancements with no impact to existing users. If an enhancement will cause a negative impact to a client, B2Gnow will notify the client and work with them to mitigate any issues.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
8.4 CUSTOMER SERVICE		
8.4.1	Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include: • Quality assurance measures; • Escalation plan for addressing problems and/or complaints; and • Service Level Agreement (SLA).	B2Gnow has a long reputation of providing excellent customer service to all clients. This is most evident in our lifetime client retention rate of 99%. B2Gnow provides unlimited customer support via email, system & phone. All support inquiries are logged and the majority resolved within one hour or less. B2Gnow standard Service Level Agreement (SLA) outlines standard support response times and escalations. Our customer support manager reviews support ticket resolutions for accuracy and training opportunities. Please review a copy of our standard SLA for additional details.
8.4.2	Offeror must describe its ability to comply with the following customer service requirements: a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current. b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones. c. Customer Service Representative will respond to inquiries within one business day. d. You must provide design services for the applicable categories. e. You must provide Installation Services for the applicable categories.	Yes; B2Gnow can assign one lead representative for each entity that executes a Participating Addendum. Contact info will be kept current. The B2Gnow support team is fully staffed Monday through Friday 8am EST to 6pm PST. Clients are also provided with an emergency after hours and weekend support contact information. Our support team will respond to all inquiries within one business day. B2Gnow typically resolves support inquiries within one hour. Not applicable. Yes; B2Gnow offers comprehensive implementation services for our system.

#	Requirement	B2Gnow Response
8.5 SECURITY OF INFORMATION		
8.5.1	Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.	B2Gnow encrypts all data both in-transit and at rest. B2Gnow maintains a robust cyber security that meets industry standards. In addition to holding and protecting client data, B2Gnow will adhere to each client's specific data disposal requirements. At contract end, B2Gnow will provide a client with a complete copy of its data before permanently deleting all data from the system.
8.5.2	Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.	The B2Gnow system is currently being utilized by over 220 public sector agencies, each with its own specific laws regarding data privacy and security. The B2Gnow system was designed with powerful configurability to allow the system to adhere to the unique data privacy and security needs of each client.
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.	B2Gnow has strict internal policies regarding access to Purchasing Entity data. B2Gnow staff will only access client data in response to a client support request. Limitations to client data access are defined in our standard Service Level Agreement. The B2Gnow system maintains detailed audit logs that track all access to client data for verification.
8.6 PRIVACY AND SECURITY		
8.6.1	Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D , including supporting the different types of data that you may receive.	B2Gnow currently fully complies with NIST SP800-145 and is committed to maintaining compliance with NIST and all other relevant industry standards related to the Scope of Services in Attachment D.
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.	B2Gnow utilizes CIS standards for service hardening and and FIPS-140 standards for data encryption. Due to the nature of our application most of the other listed standards are not applicable.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
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.	Please see B2Gnow's Security Management Plan (SMP) included in Appendix A.
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).	B2Gnow takes client data confidentiality very seriously. All B2Gnow staff must pass background checks and sign non-disclosure agreements. B2Gnow staff is trained to only view client data during the course of providing technical support to the client. No other client data access is permitted. The B2Gnow system maintains a complete audit trail of all system access. B2Gnow managers run periodic reports to review client data access and identify any unauthorized access. Unauthorized data access is grounds for immediate termination. B2Gnow support staff can only access system data from their desktop computers. They do not have access via mobile devices.
8.6.5	Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.	B2Gnow's hosting partner – Amazon Web Services (AWS) – is SSAE 16 SOC 1, 2, & 3 and FedRamp compliant. B2Gnow has begun the SOC 2 audit process and anticipates completion by year-end.
8.6.7	Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.	Yes; The B2Gnow application's security model supports restricting visibility of data and documents to specific users or groups of users.
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.	Although the system has never had a security incident that B2Gnow has identified, the B2Gnow Security Management Plan includes an Incident Response Process. As described in the Monitoring section, it is B2Gnow's policy to act proactively and respond immediately to any potential threat. Doing this has enabled B2Gnow to avoid security issues in over a decade of operations. The first step regarding a security incident is to identify it. As stated in the Monitoring section above, B2Gnow maintains system logs that record all activity. This includes checking for unusual activity from an incoming IP address. The system also monitors

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
		frequency and type of activity. If an external system attempts to connect to B2Gnow at a rate that would be impossible for a human user (e.g. more than three page views every second), B2Gnow will automatically log the attempt and block further access to that system. If there is a security breach, it will appear in the system logs that are continuously monitored. In accordance with the organization's breach and notification policies, B2Gnow shall be responsible for complying with the provisions of the organization's policy with respect to any private information (as defined in the policy) received by B2Gnow under this project (Private Information) that is within the control of B2Gnow. In the event of a breach of the security of the System (as defined by the policy), the following Incident Response Process will go into effect: • B2Gnow shall immediately commence an investigation, in cooperation with the organization, to determine the scope of the breach and restore the security of the System to prevent any further breaches. • B2Gnow shall also notify the organization of any breach of the security of the System immediately following discovery of such breach. • Except as otherwise instructed by the organization, B2Gnow shall, to the fullest extent possible, first consult with and receive authorization from the organization prior to notifying any individuals, relevant organization departments/agencies/boards, the State's Attorney General or any consumer reporting agencies of a breach of the security of the System or concerning any determination to delay notification due to law enforcement investigations. • B2Gnow shall be responsible for providing the notice to all such

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
		required recipients and for all costs associated with providing such notice. • Nothing herein, shall in any way impair the authority of the organization to bring an action against B2Gnow to enforce the provisions of its policy or limit B2Gnow's liability for any violations of the policy.
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.	B2Gnow's infrastructure partner – Amazon Web Services (AWS) – maintains extreme physical security of its hosting facilities. Non-AWS staff not permitted to access their data centers. In addition, B2Gnow maintains multiple firewalls to isolate the file, application, processing, and database server zones.
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).	Please refer to B2Gnow's Standard Service Level Agreement (SLA) and Security Management Plan (SMP).
8.6.11	Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.	As a condition of employment all B2Gnow employees must pass an initial, as well as bi-annual background checks. B2Gnow employees are only permitted to access client data at the request of the client for support purposes. All system activity and data access is logged for audit purposes.
8.6.12	Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.	Please refer to the Data Security, Transaction Security, Identity Access Management Security, Physical Security and Operating System Security sections of the B2Gnow Security Management Plan (SMP) included in Appendix A.
8.6.13	Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.	Not applicable. The B2Gnow system does not require, transact, or maintain any Cardholder data.

#	Requirement	B2Gnow Response
8.7 MIGRATION AND REDEPLOYMENT PLAN		
8.7.1	Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.	At contract completion B2Gnow will provide the Purchasing Entity with a complete copy of its data in a mutually agreed upon electronic format. The data will be encrypted in transit and provided in a mutually agreed upon method (FTPS, DVD, etc.). No data will be deleted from the system until the Purchasing Entity confirms receipt and validation of the data. The B2Gnow SLA continues to apply to the system and data during this period.
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.	B2Gnow's standard SLA states that at contract completion B2Gnow will provide the Purchasing Entity with a complete copy of its data in a mutually agreed upon electronic format. No data will be deleted from the system until the Purchasing Entity confirms receipt and validation of the data. The B2Gnow SLA continues to apply to the system and data during this period.
8.8 SERVICE OR DATA RECOVERY		
8.8.1	Describe how you would respond to the following situations; include any contingency plan or policy. a. Extended downtime. b. Suffers an unrecoverable loss of data.	B2Gnow has been providing a SaaS solution in the public sector for over thirteen years and has never experienced any of the following circumstances. B2Gnow maintains complete redundancy in every aspect of our infrastructure to prevent downtime. If our primary data center is inaccessible we have the ability to quickly route traffic to one of two backup data centers. We replicate data across all three data centers in near real-time, so no data should be lost. B2Gnow replicates data across three data centers in near real-time. In addition, we maintain periodic backups to a different location. If somehow data is lost, B2Gnow can recovery to the last known good copy of data and notify our clients of the date/time of the data loss, so they can re-enter the missing data.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
	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).	In the event of a system failure due to infrastructure B2Gnow can quickly direct system traffic to one of our two backups data centers. If a system failure was due to a software issue B2Gnow can quickly rollback to the previous software release. B2Gnow's redundant architecture allows us to easily recover and restore data within 4 business hours of a severe outage. B2Gnow supports an RPO of less than 4 hours and an RTO of less than 12 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.	B2Gnow replicates production data to two backup data centers in near real-time. In addition, periodic (daily, weekly, monthly) backups are maintained at a fourth data center. Amazon Web Services (AWS) allows us to maintain copies of server instances and easily spool up additional instances as needed. B2Gnow maintains backup across four geographically dispersed AWS data centers. B2Gnow maintains a primary AWS data center, two system backup data centers, and a fourth for periodic data backups.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
8.9 DATA PROTECTION		
8.9.1	Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.	B2Gnow uses the strongest encryption products available to protect customer data and communications. All data is encrypted both in transit and at rest. For example, the lock icon in the browser shows that 100% of data is encrypted with AES 256-bit encryption while in transit between server and client Internet browser. Passwords, financial information, and other confidential data are encrypted immediately upon receipt and stored in the database. This confidential data at rest is encrypted using the Triple-DES algorithm of Information Security Corporation's SecretAgent encryption product, which is FIPS 140-2 certified.
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.	B2Gnow is willing to sign any relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect client data.
8.9.3	Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.	All data entered into the B2Gnow system is 100% owned by our clients. B2Gnow maintains no rights to client data and will only disclosure client data upon written request from our client. B2Gnow will never resell or otherwise redistribute any data received as a result of this RFP.
8.10 SERVICE LEVEL AGREEMENTS		
8.10.1	Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.	Yes; Certain aspects of B2Gnow's standard Service Level Agreement are 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.	A copy of B2Gnow's standard Service Level Agreement has been included in Appendix A.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
8.11 DATA DISPOSAL		
	Specify your data disposal procedures and policies and destruction confirmation process.	Upon contract completion B2Gnow will provide the Purchasing Entity with a complete copy of their data in a mutually agreed upon electronic format. Upon confirmation, B2Gnow will run a script to delete the Entity's data from all applicable database tables. Once the deletion is complete, the script will reindex all database tables. B2Gnow System Administrators will run a set of reports to verify that all data has been deleted and is no longer accessible, with written confirmation to the Purchasing Entity.
8.12 PERFORMANCE MEASURES AND REPORTING		
8.12.1	Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.	B2Gnow guarantees system reliability and availability of 99.9% or greater. Over the past year B2Gnow has been at 100% availability.
8.12.2	Provide your standard uptime service and related Service Level Agreement (SLA) criteria.	B2Gnow guarantees system reliability and availability of 99.9% or greater. Please see our standard Service Level Agreement (SLA) for additional detail.
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.	B2Gnow provides our clients with unlimited technical support. B2Gnow's technical support team is available via phone, email, and through the system from 8am EST until 6pm PST on business days. Clients are also provided with after hours emergency contact information.
8.12.4	Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.	B2Gnow's SLA can provide a provision for annual service fee credits if incident response times and incident fix times are not met.
8.12.5	Describe the firm's procedures and schedules for any planned downtime.	B2Gnow's redundant system architect allows the majority of system updates to be completed with zero downtime. If planned downtime is required, it would be communicated to all clients, via system portal and email, at least 72 hours in advance and is typically scheduled for a weekend when system activity is minimal.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
8.12.6	Describe the consequences/SLA remedies if disaster recovery metrics are not met.	B2Gnow's SLA can provide a provision for annual service fee credits or contract termination if disaster recovery metrics are not met.
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.	Please see sample performance reports included in Appendix A. Certain performance reports are available in real-time in the system. Performance reports provided from 3rd-party services can be provided monthly.
8.12.8	Ability to print historical, statistical, and usage reports locally.	These are standard reports that our clients can print from the system at any time.
8.12.9	Offeror must describe whether or not its on-demand deployment is supported 24x365.	The B2Gnow system is available 24 x 365.
8.12.10	Offeror must describe its scale-up and scale-down, and whether it is available 24x365.	The B2Gnow system is available on-demand 24 x 365 with no scale-up or scale-down.
8.13 CLOUD SECURITY ALLIANCE		
	Describe and provide your level of disclosure with CSA Star Registry for each Solution offered. a. Completion of a CSA STAR Self-Assessment. (3 points) b. Completion of Exhibits 1 and 2 to Attachment B. (3 points) c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points) d. Completion CSA STAR Continuous Monitoring. (5 points)	B2Gnow has completed a CAIQ and included it in Appendix A.
8.14 SERVICE PROVISIONING		
8.14.1	Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.	The nature of Diversity and Vendor Management Software does not typically include emergency or rush service provisioning. However, B2Gnow has a long track record of meeting and exceeding the implementation timelines desired by our clients.
8.14.2	Describe in detail the standard lead-time for provisioning your Solutions.	The B2Gnow system contains thousands of configuration settings and we have a standard implementation methodology to bring up new clients. Our typical implementation timeline is 12 – 16 weeks.

#	Requirement	B2Gnow Response
8.15 BACK UP AND DISASTER PLAN		
#	Requirement	B2Gnow Response
8.15.1	Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.	Yes; The B2Gnow system includes the ability to apply legal retention periods and disposition by agency to comply with its purchasing and/or legal requirements.
8.15.2	Describe any known inherent disaster recovery risks and provide potential mitigation strategies.	B2Gnow has partnered with Amazon Web Services (AWS) to provide our technical infrastructure. AWS is known for its reliability. B2Gnow has a primary AWS hosting facility and two backup facilities. Data is replicated across all three systems in near real-time to prevent any data loss in the event of a disaster at our primary data center, with an additional backup dataset stored at a fourth data center.
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.	B2Gnow has partnered with Amazon Web Services (AWS) to provide our technical infrastructure. B2Gnow has a primary AWS hosting facility and two backup facilities. Data is replicated across all three systems in near real-time to prevent any data loss in the event of a disaster at our primary data center, with an additional backup dataset stored at a fourth data center. The data centers are geographically dispersed with industry leading redundancy, failover capabilities, and the ability to run enterprise applications independently in the event any facility is lost.
8.16 HOSTING AND PROVISIONING		
8.16.1	Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.	B2Gnow is a multi-tenant, SaaS solution, utilizing Amazon Web Services (AWS) for its technical infrastructure. AWS provides a sophisticated dashboard and tools for provisioning additional instances and capacity. The system is continually monitored for performance and additional resources can be provisioned dynamically or on-demand as necessary to maintain system performance.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
8.16.2	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).	As a hosted SaaS solution B2Gnow manages the entire technical infrastructure to maximize system reliability, performance, and availability. B2Gnow system administrators, not Purchasing Entity staff, will manage the deployment of new servers, server images, and additional storage space. The system includes standard monitoring tools and reports that can be accessed by authorized personnel of each jurisdiction.
8.17 TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE)		
8.17.1	Describe your testing and training periods that your offer for your service offerings.	Prior to purchase, B2Gnow can provide prospective clients with detailed demonstrations and access to an evaluation system. After purchase, B2Gnow will provide clients with access to a test system that will be fully configured to the requirements of that client. Clients will have access to this test and training environment for the length of our engagement, including after implementation.
8.17.2	Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.	After purchase, as part of the implementation process, B2Gnow will provide clients with access to a test system that will be fully configured to the requirements of that client. Clients can use this testing environment to validate that the B2Gnow system meets or exceeds all of their functional and technical requirements. The length of the testing period is flexible to the needs of the client.
8.17.3	Offeror must describe what training and support it provides at no additional cost.	Included in our annual service fee is unlimited web-based training and technical support at no additional cost. Refer to the Technical Response section of this proposal for additional details.

State of Utah / NASPO ValuePoint
SK18008 – Master Agreement for Cloud Solutions



#	Requirement	B2Gnow Response
8.18 INTEGRATION AND CUSTOMIZATION		
8.18.1	Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.	Yes; B2Gnow offers a standard 3rd-party data integration methodology. B2Gnow has completed over 400 data import and export integrations with dozens ERP, financial management, project management, and vendor management systems. We offer standard pricing for integration with 3rd-party systems.
8.18.2	Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.	The B2Gnow system includes thousands of configurable settings. This allows us to configure and personalize our system to meet the specific requirements of an agency without the need for costly and time-consuming customizations. This includes a branded login portal, customer logos, and branded notification templates. While we do have the ability to customize the solution for a client, it is rare.
8.19 MARKETING PLAN		
8.19	Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.	If awarded a NASPO ValuePoint contract B2Gnow plans to market our solution to participating entities through: 1. A dedicated website to highlight our ValuePoint relationship; 2. Outbound marketing campaign to participating entities; 3. Webinar series for participating entities; 4. 4) Road trips across the country with invitations to participating entities.

#	Requirement	B2Gnow Response
8.20 RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS		
8.20	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.	B2Gnow provides our SaaS solution with a comprehensive one-time setup fee and annual service fee. The setup and annual service fees are all-inclusive of everything a Purchasing Entity will need to successfully implement and utilize the B2Gnow system. In the situations where a Purchasing Entity requires additional services from B2Gnow, these are provided in a detailed proposal and Statement of Work, and can include: • Data entry • Data migration or integration • Custom report development • System customizations • Program consulting & process optimization • Supplemental onsite training • Supplemental project management services
8.22 SUPPORTING INFRASTRUCTURE		
8.22.1	Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.	The only requirement to access the B2Gnow system is Internet access on a device with a common web browser. B2Gnow supports all common web browsers at least three version back. No downloads, cookies, plug-ins, or other third-party software is needed top access and utilize the B2Gnow system.
8.22.2	If required, who will be responsible for installation of new infrastructure and who will incur those costs?	Not applicable.

APPENDIX A – ADDITIONAL B2Gnow INFORMATION

Additional information about B2Gnow Diversity and Vendor Management software is included in this proposal.

Product Information & Samples

- B2Gnow Security Management Plan
- Standard B2Gnow Service Level Agreement
- Sample system performance reports
- CSA Star Consensus Assessments Initiative Questionnaire (CAIQ)



Service Level Agreement



SYSTEM ACCESS FOR USERS IS 24/7

B2Gnow is a 100% web-based system with guaranteed availability of at least 99.9%. As a result, the system is available 24/7 from anywhere with Internet access. Use of the B2Gnow system does not require any downloads, plug-ins, or cookies for either the organization staff or their contractors/vendors to access.

DATA OWNERSHIP AND RETENTION

The organization retains complete ownership rights to all data added to the system by its staff whether through manual entry or data interfaces. B2Gnow maintains no rights to the organization's data and will only disclose or release data on explicit instruction from approved organization staff.

Organization data will remain in the system for the duration of our engagement or until B2Gnow is instructed to archive or delete historic data. B2Gnow will comply with any data retention, deletion, or archive requirements that the organization is subject to.

The organization can export its data from the B2Gnow system at any time without assistance from B2Gnow staff. Furthermore, at the end of our engagement B2Gnow will provide the organization with a complete electronic copy of all its system data and notify the organization of its right to instruct B2Gnow to permanently destroy any and all archived or current data in accordance with the organization's retention and disposition requirements.

SECURITY CAPABILITIES

Software and System Security

B2Gnow has implemented industry-standards for security access control including user specific logins, complex passwords, password expiration, concurrent logins (not permitted), and the ability to restrict or permit access based on IP range.

B2Gnow protects against unauthorized data access on several levels. Each individual accessing the system is required to have a unique login and password. Passwords can be set to automatically expire on a periodic basis requiring users to change their passwords using "strong" password standards. However, end-users will be able to change their password more frequently. The system enforces complex password requirements and does not permit concurrent logins. The system incorporates a triple-tier firewall architecture that includes spam and virus blockers and is monitored 24/7, both internally and by 3rd-party firms, for intrusion detection and unauthorized access. Any unauthorized breaches in security will be reported to the organization immediately. A detailed account of any security breach, with remediation measures undertaken by B2Gnow, will be provided to sufficiently allow the organization to determine its future risk and current liability, if any. B2Gnow implements Strong Secure Sockets Layer Https Encryption for Network Security, which also includes the transmission of the organization's data using secure File Transfer Protocol (FTP) sites

B2Gnow has never experienced unauthorized access to the system or data during our entire history.

B2Gnow prevents inadvertent deletion of data in several ways. The system will not permit records that are associated with other data to be deleted. Secondly, the system utilizes a two-phase commit process, and asks the user to verify the deletion before completing the process. The B2Gnow system administrator has the ability to restore deleted data, except where explicitly instructed to permanently delete records per the organization's data retention and disposition requirements.

The data stored within the B2Gnow system will be secured and access rights appropriately limited to those users (B2Gnow and organization representatives) who have been granted access. Any administrative access to the organization's data by employees of B2Gnow will be logged.

Security at Physical Locations

Primary and all secondary data centers, including archival centers where the organization's data may reside, will be in an electronically secure facility, within the United States, that automatically tracks employee access, and non-employee access, who are authorized to perform service and support under an existing service agreement. Access to the secure physical facility will be tracked 24 hours per day, 7 days per week. An electronically generated log reporting facility access will be available to the organization on demand within 72 hours.

HOSTING, SYSTEM BACK-UP, AND DISASTER RECOVERY

As a hosted SaaS solution B2Gnow guarantees availability of 99.9%. We have always exceeded this guarantee and typically operate above 99.9%. B2Gnow maintains redundancy at every level of our architecture. We utilize multiple co-location facilities (each with redundant power, HVAC, & bandwidth), load balancers, redundant servers & devices at each node, database mirroring, and disk-disk-tape backup.

B2Gnow utilizes third-party services to monitor system available from multiple locations around the United States at least once every five minutes. If the system experiences an outage, B2Gnow system administrators and senior management are notified immediately.

B2Gnow's backup procedure has been designed to guarantee that no more than 4 hours of data would be lost due to a complete system failure, which has never occurred in the system's history. If a primary database server should fail, the system will automatically direct traffic to the redundant server. If both servers fail, the production database is backed up on disk to a separate server every four hours. Additionally, an encrypted backup is written every 24 hours and secured offsite weekly.

In the case of catastrophic system failure we maintain a disaster recovery environment available for rapid switchover and at least three additional training, testing, and development environments with full functionality that could be utilized at any time.

B2Gnow will maintain a disaster recovery environment in place that includes, at no additional cost to the organization, the system and its data. The disaster recovery environment will be tested at least once a year to verify the accuracy and availability of the DR system in the case of production system failure.

SOFTWARE UPDATES

The organization is entitled to all standard software updates made to the purchased modules that are a part of B2Gnow's general software update program. These updates are defined based on feedback from all customers. The organization will be made aware of new updates through release notes provided on the B2Gnow dashboard, the system bulletin board, and/or through email alerts. All updates are implemented in such a manner to optional to all clients and are deployed initially in an "off" state. Software enhancements are released at a minimum on a quarterly basis.

The organization may request new enhancements at any time by contacting support. An enhancement request form must be completed and submitted to B2Gnow's technical architect. B2Gnow will provide a scope of effort, cost proposal, timeline, and initial prioritization for the organization to review. In general, B2Gnow will not charge for enhancements if multiple clients are asking for a similar enhancement and the implementation timeframe can be agreed upon by all parties.

CUSTOMER SUPPORT

B2Gnow offers comprehensive customer support services to meet our customers' needs.

Types of Support

B2Gnow's Customer Support includes many different support options:

- Online support through the system and email
- Telephone support
- User training webinars
- User manuals and quick-guides

The primary method of contacting Customer Support is through the system. The B2Gnow system has a built in support capture mechanism that collects relevant information and routes it immediately to the support team, resulting in the fastest response. An integrated Help Desk module identifies the user to support staff and permits the first available team member to review and respond to the query.

Users can ask any type of question; however, queries regarding the organization's procurement policies received by B2Gnow Customer Support will be assigned to the appropriate organization staff member. Organization staff users are able to use the Help Desk module to respond to queries, which then maintains a history of all support contact.

A dedicated email address will be configured to collect email support queries and automatically log them into the Help Desk module. Once logged, they are viewed and answered in the same manner.

Organization staff can contact support by telephone for priority issues. Vendors are encouraged to contact support through the system or email for fastest response, but B2Gnow support staff are authorized to respond to vendors by phone if necessary to resolve an issue.

B2Gnow offers regular training webinars to all staff and vendor users. Users can register for a class and attend while sitting at their computer. User manuals and quick-guides are provided in PDF format for download.

Contacting Support

B2Gnow support contacts:

Online:	Click any "Customer Support" link in the system
Email:	To be determined
Phone:	To be determined
Toll-free Fax:	866-892-2913

Support queries submitted outside these protocols will be redirected to the B2Gnow Support Team. Emergency contact information will be provided during implementation to key organization staff.

Hours of Availability

B2Gnow's customer support help desk is available during the hours listed below. Times are for standard support; additional hours of support are available for enhanced levels of service on a negotiated case-by-case basis.

Customer Support: Based on organization's time zone
Technical Support: Based on organization's time zone

Normally, calls and emails that are received after hours are responded to the following business day. Priority 1 calls, once logged during business hours, are generally worked through to completion even outside of normal business hours. If the organization desires to contract after-hours priority coverage, B2Gnow provides an "after hours phone number" on a rotating basis with Support Center Personnel, so that B2Gnow can assure a timely response on Priority 1 and Priority 2 problems (two hour response time, seven days a week).

Response Times

The following table provides technical support response metrics during normal business hours (8am to 5pm Central Time, Monday through Friday).

Service Item	Goal	Maximum
Internal System Response	Problem Reports and Callback Requests will be responded to within 2 hours.	Problem Reports and Callback Requests will be responded to within 48 hours.
Voice Mail Response	Voice mail will be responded to within 2 hours.	Voice mail will be responded to within 48 hours.
Email Response	Email will be responded to within 2 hours.	Email will be responded to within 48 hours.

The stated metrics are B2Gnow's goals and maximums. However, our performance in reaching these metrics may be affected by factors outside our control (defined in the B2Gnow SLA Exclusions section). Support queries submitted outside of the accepted protocols (designated support email address, in-system Help Desk tool, support phone number, support fax number) will be redirected to the B2Gnow Support Team. Measurement of response time will be measured only upon receipt of the query by the Support Team. Queries submitted to the Support Team that are ultimately assigned to organization staff for resolution will not be counted towards SLA compliance. For queries received out of normal business hours, tracking time will commence at the start of the next business day (8am Central Time, Monday through Friday).

System problems communicated to B2Gnow will be immediately sent to the B2Gnow technical support team for review and action. The B2Gnow technical support team will review and act upon any system problems reported to it. It will be routed either to the development team (if it is a software issue), or the system administration team (if a hardware, hosting, or network issue). The product's lead developer is available to the support staff and the system administration team to ensure fast technical resolutions.

Furthermore, automated tracking of customer incidents and support requests is incorporated into the B2Gnow software. Users can submit "Problem Reports" and support requests directly into the system, which will be viewable by system administrators, Help Desk staff, and B2Gnow support team members. Once the issue is resolved, a response can be sent to the original user, providing an audit trail of action. The user can view the response and the action taken to resolve the issue. If necessary, the user can continue interaction with the support team.

Any errors within the system are automatically logged with an email alert sent to the B2Gnow support team. Typically, the support team is aware of an issue before it is reported.

User Responsibilities

Information. A user's problem report to B2Gnow must contain all pertinent information on an approved problem report template, in English, including user's name and location, B2Gnow Software/Product Release number or B2Gnow hosted solution name, client or server operating system/version, hardware platform, problem description, log files/test case and problem severity. User must execute diagnostic routings if provided by B2Gnow and inform B2Gnow of the results. User must also verify the existence of a problem and provide the conditions in which the problem may be duplicated.

Technical Contact. For the period B2Gnow is working the user's problem, the user shall provide a technical contact who is familiar with the problem and the user's environment.

Remote Access. User shall provide remote access when required by B2Gnow to analyze a problem.

Priority & Severity Levels

B2Gnow will diligently work for the prompt resolution of defects and errors in the software, hardware, or connectivity of the B2Gnow Service. System problems can be submitted by phone, email, or internally within the system (Problem Report, Callback Request, and Administrator Message functions).

The customer is best able to assign a severity level to a problem; however, B2Gnow Technical Support will ask questions to assure the right resources are assigned. When reporting a problem or updating the status of an incident, customers should always call B2Gnow's main support number rather than a particular B2Gnow employee. If you have a Severity 1 or 2 problems with your system, please inform the first representative when you call in so your problem will be escalated to the right person as quickly as possible.

B2Gnow will respond to and complete correction of errors, defects and malfunctions, in accordance with the following schedule:

Priority 1/Severity 1: An error isolated to the B2Gnow software that renders system inoperative or causes the product to fail catastrophically; e.g. major system impact, system down.

B2Gnow will make an initial response to a Severity 1 normal maintenance call within two hours after receipt. Severity 1 calls will be handled on a 24x7 basis. B2Gnow will use reasonable efforts to provide a fix, work around or to patch a Severity 1 defect within twenty-four hours after the problem is replicated by B2Gnow and confirmed as a defect.

Priority 2/Severity 2: An error isolated to the B2Gnow software that substantially degrades the performance of the product or materially restricts business; e.g. system hanging, some functionality not accessible.

Provided that the maintenance call is received within B2Gnow's normal maintenance hours, B2Gnow will make an initial response to a Severity 2 maintenance call within four hours after receipt. B2Gnow will make reasonable efforts to provide a fix or work around for a Severity 2 defect within three business days.

Priority 3/Severity 3: An error isolated to the B2Gnow software that causes only a minor impact on use of the product; e.g. system slowdown.

Provided that the maintenance call is received within B2Gnow's normal maintenance hours, B2Gnow will make an initial response to a Severity 3 maintenance call within twenty-four hours after receipt. B2Gnow will make reasonable efforts to provide a fix or work around for a Severity 3 defect within five business days.

Priority 4/Severity 4: A reported anomaly to the B2Gnow software, which does not substantially restrict the use of one or more features of the licensed product to perform necessary business functions.

Provided that the maintenance call is received within B2Gnow's normal maintenance hours, B2Gnow will make an initial response to a Severity 4 maintenance call within forty-eight hours after receipt. B2Gnow will make reasonable efforts to identify a resolution to a Severity 4 defect within thirty days and to incorporate Severity 4 fixes into the next release of the product.

Priority 5/Severity 5: Enhancement request.

Provided that the maintenance call is received within B2Gnow's business hours, B2Gnow will make an initial response to a Severity 5 maintenance call within five business days after receipt. Severity 5 issues will be dealt with on a case-by-case basis.

Errors within the system are automatically logged with an email alert sent to the B2Gnow support team. Typically, the support team is aware of an issue before users report it. Team members will proactively monitor the system to analyze user behavior and system response.

TRAINING

B2Gnow provides ongoing training for staff and vendor users as part of its standard webinar training program. Users can sign up and attend relevant training classes, which is useful for new staff or users seeking a refresher on the system's capabilities. This web-based training is included at no additional cost as part of the annual service fee. Onsite training is also available, but is billable per the contract.

WARRANTY

The B2Gnow system is warranted to be free of technical errors for the entire duration of the contract.

SYSTEM MAINTENANCE

On a scheduled basis, B2Gnow performs maintenance on the software system and technical environments. System upgrades are completed at the same time. The system is typically available for most or all of the maintenance period; if the system is expected to be offline for any period of time, a system maintenance web page is displayed to users.

System maintenance:	Thursday/Friday, 9pm to 5am (Pacific Standard Time)
Database optimization:	Saturday/Sunday, 9pm to 5am (Pacific Standard Time)

B2Gnow will notify the organization of planned infrastructure changes that will impact system access at least 48 hours prior to the change.

SYSTEM MONITORING

B2Gnow utilizes multiple 3rd-party services (Site 24x7, Alertra, Pingdom, and Alerts) to monitor system availability and performance from cities across the country. In addition to immediately alerting our staff to system issues, these services track B2Gnow system availability.

System availability is monitored in five-minute intervals and B2Gnow guarantees service uptime of at least 99.9%. Scheduled maintenance and downtime is excluded for purposes of this calculation. Monthly uptime percentage is calculated by taking the total number of applicable minutes in a calendar month minus the total number of minutes of Downtime, all divided by the total number of applicable minutes in that calendar month. This is reflected in the following formula:

$$\frac{\text{Total number of applicable minutes in the month} - \text{Total minutes of Downtime in the month}}{\text{Total number of applicable minutes in the month}}$$

For SLA monitoring and reporting, B2Gnow will use data from Site24x7.com. The monitoring service will determine availability and response performance of the B2Gnow SaaS system by polling at least once every five minutes from three locations across the United States. The information will be aggregated automatically by the Site24x7.com service to account for public Internet issues (outside of the control of B2Gnow) to provide a quantitative measure of availability and response performance as provided by the B2Gnow SaaS system. B2Gnow can, at its discretion, poll availability more frequently.

B2GNOW SLA EXCLUSIONS

The Service Level Agreement does not apply to any unavailability, suspension or termination of the B2Gnow System, or any other B2Gnow System performance issues:

1. caused by factors outside B2Gnow's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of the B2Gnow System;
2. that result from any actions or inactions of the organization or any third party not within B2Gnow's direct control;
3. that result from the organization's equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within B2Gnow's direct control);
4. caused by use of the System after B2Gnow advised a user of the System to modify his/her use of the System and the user did not modify his/her use as advised;
5. attributable to the acts outside of normal system use or omissions of the organization or its employees, agents, contractors, vendors, or users.