STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 1

CONTRACT #: AR2501

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and Contact Solutions, LLC (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

The Master Agreement Attachment A Sections 8, 16, and 17 are replaced by the terms on the attached Exhibit 1. All other terms and conditions of the original agreement remain in full force and effect.

Effective Date of Amendment: February 3, 2017

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

CONTRACTOR		**STATE OF UTAH**	
Contractor's Signature	Date	Kent Beers Director	Date
	Digitally signed by Lynn Machleit, VP Finance Date: 2017.02.17 12:17:51 -05'00'	State of Utah Division of Purchasing	2.17.17
Contractor's Name (Print) **CONTACT SOLUTIONS, LLC (Vendor # VC205718; Commodity Code #920-05)**			
11950 Democracy Drive, Reston VA 20190			
Title (Print)			

Purchasing Agent	Phone #	e-mail	**Contract #**
Spencer Hall	801-538-3307	spencerh@utah.gov	AR2501

Digitally signed by Beasley, Lynn
DN: dc=com, dc=Verintsystems, dc=Corp, dc=Verint, ou=Regions, ou=AMER, ou=Sites, ou=ATL, ou=Users, ou=User accounts, cn=Beasley, Lynn
Date: 2017.02.17 12:12:38 -05'00'

Exhibit 1

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

b. Non-Disclosure. The Parties 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. The Parties shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. The Parties shall use commercially reasonable efforts to assist in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, each Party shall advise Contractor, Purchasing Entity, applicable Participating Entity, and the Lead State immediately if the Party 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 the Party shall at its expense cooperate with the affected Party in seeking injunctive or other equitable relief in the name of the affected party against any such person. Except as directed by the 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. The Parties acknowledge that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to the affected Party that is inadequately compensable in damages. Accordingly, the affected Party 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. The Parties acknowledge and agree that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity, Participating Entity, and Contractor 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.

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 Participating Addendum.

b. The minimum acceptable limits shall be as indicated below, for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, 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) Data Breach, Privacy, Cyber Liability and E&O are included in the Professional Liability policy (detailed below).

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 Verint's Professional Liability policy (including E&O, Cyber, Network, Privacy Liabilities) is "per claim" with a limit of $10,000,000 that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies and shall be fully responsible for payment of all applicable deductibles. 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 notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any 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.

d. 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); 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.

e. Coverage and limits shall not limit nor expand Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

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

Contract # AR2501

STATE OF UTAH COOPERATIVE CONTRACT

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

Contact Solutions, LLC		
Name		
11950 Democracy Drive		
Address		
Reston	VA	20190
City	State	Zip

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

Contact Person Timothy Grimes Phone #703-782-1416 Email tgrimes@contactsolutions.com
Vendor #VC205718 Commodity Code #920-05

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

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

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

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

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

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

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

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

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

CONTRACTOR

Contractor's signature — Date: 9/22/2016

Timothy Grimes, SVP Sales
Type or Print Name and Title

STATE

For Director, Division of Purchasing — Date: 9.26.16

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

(Revision 16 June 2016)

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

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

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

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

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

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

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

10. Defaults and Remedies

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

(1) Nonperformance of contractual requirements; or

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

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

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

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

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

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

(1) Exercise any remedy provided by law; and

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

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

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

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

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

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

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

13. Indemnification

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

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

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

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

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

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

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

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

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

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

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

16. Insurance

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

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

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

(2) CLOUD MINIMUM INSURANCE COVERAGE:

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

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

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

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

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

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

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

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

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

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

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

19. Ordering

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

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

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

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

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

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

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

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

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

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

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

20. Participants and Scope

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26. Records Administration and Audit.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32. Transition Assistance:

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

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

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

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

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

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

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

37. Governing Law and Venue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

The limitations of liability in Section 43 will not apply to claims for bodily injury or death, Section 8, Section 13, and Section 30.

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

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

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

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

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

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

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade that is deemed to have an impact service availability and performance.

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 will ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data based on client (Purchasing Entity) and data requirements. Additionally, Contact Solutions will provide the client (Purchasing Entity) IVR SaaS performance metrics with and without whole disk encryption. This will allow a risk-based decision to be made based on system performance, business mission objectives, and encryption of data at rest security control requirements.

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

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

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
SaaS	Yes	Yes	Not at this time	Contact Solutions intends to provide Software as a Service (SaaS) via private cloud with the following subcategories. • Other – Interactive Voice Response
IaaS	(Bundled with SaaS)	(Bundled with SaaS)	N/A	
PaaS	(Bundled with SaaS)	(Bundled with SaaS)	N/A	

Contact Solutions uses the following guidance extracted from *NIST Special Publication 800-60 Volume II, Revision 1, Guide for Mapping Types of Information and Information System to Security Categories.*

Cost Proposal

In response to:

RFP CH16012 – Cloud Solutions

Submitted to:

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

Submitted by:

Michael Southworth, CEO
Contact Solutions, LLC
11950 Democracy Drive, Suite 250
Reston, VA 20190
Phone: (571) 385-1283
Fax: (703) 480-1676
msouthworth@contactsolutions.com

March 10, 2016

Contact Solutions
A VERINT Company

11950 Democracy Drive • Suite 250 • Reston, VA 20190 • P 703.480.1620 • F 703.480.1676

March 10, 2016

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

Re: RFP CH16012 – Cloud Solutions

Dear Mr. Hughes and members of the proposal evaluation committee:

Contact Solutions is pleased to present in this volume its Cost Proposal to provide Cloud Solutions to the Participating Entities involved in the NASPO ValuePoint program, and the citizens they serve.

Thank you for this opportunity.

Sincerely,

Michael Southworth, CEO
Phone: (571) 385-1283
Fax: (703) 480-1676
msouthworth@contactsolutions.com

Table of Contents

Attachment G – Cost Schedule

Solicitation Number CH16012
NASPO ValuePoint Cloud Solutions RFP

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

Software as a Service	Discount % 25
Infrastructure as a Service	Discount % N/A
Platform as a Service	Discount % N/A
Value Added Services	Discount % 25

Additional Value Added Services

Maintenance Services

Onsite hourly rate $ 225
Remote hourly rate $ 225

Professional Services

- Deployment Services — Onsite hourly rate $ 225; Remote hourly rate $ 225
- Consulting/Advisory Services — Onsite hourly rate $ 225; Remote hourly rate $ 225
- Architectural Design Services — Onsite hourly rate $ 225; Remote hourly rate $ 225
- Statement of Work Services — Onsite hourly rate $ 225; Remote hourly rate $ 225

Partner Services — Onsite hourly rate $ 225; Remote hourly rate $ 225

Training Deployment Services — Onsite hourly rate $ 225; Remote hourly rate $ 225

Price Catalog

Non-Recurring Fees (Base Configuration)

	List Price	Description
Basic Inbound IVR [1, 2, 3, 4]		
Basic Configuration - Tier 1	$23,850	– Includes 1 DNIS (can include 1 or more toll free numbers) – Up to 3 customer journeys (goals) – Single host interface, up to 2 transactions – Single unique transfer – Standard Optimization Portal with access to business hours and up two temp messages – Full standard reports (IVR call volume, host transaction, and tasks & goals reports)
Basic Configuration - Tier 2	$37,800	– Includes 1 DNIS (can include 1 or more toll free numbers) – Up to 6 customer journeys (goals) – Single host interface, up to 4 transactions – Up to 3 unique transfers – Standard Optimization Portal with access to business hours and up two temp messages – Full standard reports (IVR call volume, host transaction, and tasks & goals reports)
Basic Configuration - Custom	Assessed Individually	Labor estimate provided by Contact Solutions based on specific needs of the Participating Entity

Notes
1) Price is per application and for Inbound IVR only. Professional language fees are not included.
2) Limited to web services only. Requires accurate interface documentation provided by client.
3) Assumes single deployment of all features. Phased deployment requires custom assessment.
4) Additional functionality, capabilities or quantities beyond those identified in the Description above are considered custom and could be subject to additional fees.

Non-Recurring Fees (Additional Features and Functionality)

Incremental to Basic Inbound IVR and OPTIONAL

	List Price	Description
Miscellaneous		
Integration to payment processor	$27,000	This integration is required in the event the payment processor is not currently part of the host being used in the primary integration.
Additional Toll Free Numbers	$450	Any additional TFN's not part of the original IVR build.
Transfers to additional Contact Center	$3,600	Adding transfers to more than one contact center outlined in IVR build.
First Non English Language	20% of assessed total for the English IVR application	Price is per language based on, basic or mid-tier plus all additional IVR fees [e.g., additional goals ; includes Spanish script validation]). Includes the required TFN transfers to mirror the core IVR TFNs. Only applies to languages and/or voice recordings that already exist on our platform. This is for Touchtone applications only.
Additional Languages	$3,600	Fee for adding each additional language
Adaptive Personalization		
Adaptive Recall [1]	$30,000	ANI/Phone number assisted authentication, remember language selection, and up to two behavior based call flow changes, i.e. Callers that navigate to a balance will have the balance automatically played after a set number of calls occurs. (Main menu changes or data pushes only). These preferences are set after a predefined number of calls.
Adaptive Audio [1]	$30,000	Adaptive playback control based on speed an accuracy of user input (with 3 different voice prompt speeds). This option utilizes speech, DTMF, and ambient sound to adjust the speed, as well as additional help, of IVR prompts to better assist callers.

Notes
1) Incremental recurring Personalization Fees apply

Business Intelligence Gateway		
Business Intelligence Gateway (BIG)	Assessed Individually	Labor estimate provided by Contact Solutions based on specific needs of the Participating Entity
Adaptive Fraud		
Adaptive Fraud	Assessed Individually	Labor estimate provided by Contact Solutions based on specific needs of the Participating Entity
Outbound Fax On-demand [1]		
Standard FAX	$3,600	Faxes must be a static form with no dynamic/ variable information added to the body of the fax
Dynamic FAX	$8,100	Similar to a Standard Fax, however, dynamic/ variable information can be added to the fax, i.e. A balance can be added to the body of the fax. No more than 30 dynamic user-defined fields can be utilized.
Enhanced Dynamic FAX	$13,500	Similar to the Dynamic Fax, these faxes can contain a customized formatted document with the ability to add logos, fonts and borders. Unlimited dynamic, user-defined fields and allows for expanding length of the fax.

Notes
1) Incremental recurring Fax On-demand Fees apply for any Fax type outlined above.

Outbound Email On-demand [1]		
Static Data	$900	Predefined form. No dynamic data. Total email size limit which includes the email itself and any attachments cannot exceed 19.5 MB.
Dynamic Data	$10,800	Predefined form with the addition of up to 30 dynamic, user-defined fields. The dynamic fields are captured from the host transactions performed during the call or data dips into the host and then populated into the 30 custom columns of the email detail table.

Notes
1) Incremental recurring Email On-demand Fees apply to all email types outlined above.

	List Price	Description
Extract-Transform-Load Function for Download of Client Data		
Basic ETL	$5,400	Voice self-service typically requires that the IVR have access to customer data. Ideally the data is accessed via a series of host transactions, usually web services, as identified in the "Basic Inbound IVR" section. However, if for some reason Contact Solutions cannot be granted access to the government entity's data systems, Contact Solutions can maintain a copy of the entity's data within our own data centers. The process for obtaining and making regular updates to that copy is the ETL process. - 1 file per table - Up to 70 columns in total per file - Up to 100 bytes per column - Up to 50,000 rows per table - Comma or bar column delimiters - Daily imports will be total refresh in nature, not updates
Datafeed Function to Update Customer Data with Changes Made by Callers in the IVR		
Basic datafeed	$3,600	Voice self-service often requires that the IVR be able to make updates to customer data. Ideally the data updates would be made via a series of host transactions as identified in the "Basic Inbound IVR" section. However, if for some reason Contact Solutions cannot be granted access to the government entity's data systems, Contact Solutions can make updates, made by callers in the IVR, via the data feed process. As with the ETL process, all updates for a given period of time are provided via a data feed on a scheduled basis. Note that Basic Datafeed offering makes the data available on the Contact Solutions ftp/sftp site for retrieval by the government entity. - Data from the following sources: CDRAPP Data standard columns, CDRAPP data custom columns, AppData EXT custom columns, and/or advanced features table (name/value pairs) - Data will be extracted and inserted into the datafeed per the approved client spec - One file will be generated per day (typically for previous day's data) - Push to the Contact Solutions FTP or SFTP
Text Messaging (via SMS)		
Basic outbound SMS campaign	$31,950	Base price for one-way outbound SMS; includes up to 3 keywords (outbound messages) Includes one carrier provision fee, MMS fee and one carrier provisioning fee, CS fee, and random dedicated short code
Add two-way messaging (includes ETL and double verification)	$37,350	Add two-way messaging, includes standard words (i.e., STOP, HELP, CONFIRM, Yes, and NO); includes up to three host transactions/keywords (e.g., sending balance/BAL). Includes one carrier provision fee, MMS fee and one carrier provisioning fee, CS fee, and random dedicated short code
Optional host transaction	$5,400	Should the SMS information, eg mobile number and data fields, reside in the host integration already in place.
Customer Satisfaction Surveys (Phone-based)		
Survey [1]	$10,800	Up to five questions

Notes
1) Recurring IVR Usage Fees apply

	List Price	Description
Addition of Speech Recognition to Touchtone IVR		
Press or Say Speech	$51,300	Addresses the speech requirement found in many government RFPs to simply address the American Disability Act (ADA) without adding significantly to the development fees. It relies solely on the digits and Boolean built-in grammars and does not require a VUI designer or any custom grammars. E.g. “For balance, press or say ‘one’”. Includes the cost for 1 speech tuning session within the first 90 days of operations.
Standard Directed Dialogue	$125,550	Could potentially also be defined as Press-Or-Say except in this case we would use a VUI designer and there is a need for custom grammars. E.g. “For balance, say Balance” with a DTMF fallback of “For balance, press 1.” This category would be used more as an entry level speech application for commercial deployments or where a government program might be willing to pay for a better customer experience than the bare minimum Press-or-Say approach. .Includes the cost for 1 speech tuning session within the first 90 days of operations.
Advanced Directed Dialogue	$167,400	Includes the cost for 2 speech tuning session within the first 90 days of operations.
Text-to-Speech		
Add TTS to Touchtone IVR	$5,400	Includes up to three data elements (e.g., full address [including street, state, city, zip] equals one data element)
Computer to Telephony Integration (CTI)		
Basic CTI	$18,000	Transfer to single contact center, up to 2 data elements, for new IVRs or application builds only. This also includes 10 hours of technical consulting
Outbound Calling Campaigns		
Basic call campaign (playback)	$15,300	Base price for Outbound Call Campaigns. This includes up to 1 unique dial/flat file. Requirements for additional data or data/flat file's be required, each will be assessed separately and may incur additional costs based on complexity of the requirement
Add bridge to agent	$2,700	Requires transfers; transfer fees will be passed through to client
Add bridge to agent with input	$5,400	Requires transfers; transfer fees will be passed through to client
Add bridge to survey	$5,400	Requires transfers; transfer fees will be passed through to client
Optional host integration	$10,800	Includes 1 host transaction with up to 2 data elements per transaction.

Recurring Fees (Base Configuration)

Touchtone III per Minute Fees[1]	
0-1M minutes per month	$0.046
1M-5M minutes per month	$0.038
5M-10M minutes per month	$0.029

Notes:
1) Voice telecommunications carrier fees not included in IVR fees

Recurring Fees (Additional Features and Functionality)

Incremental to Basic Inbound IVR and OPTIONAL

Speech Recognition per Minute Fees[1, 2]	
0-1M minutes per month	$0.018
1M-5M minutes per month	$0.015
5M-10M minutes per month	$0.012

Notes:
1) Speech recognition fees are incremental to Touchtone IVR fees
2) Does not include natural language which requires separate pricing

Adaptive Recall per Call Fees	
250K-1M calls per month	$0.007
1M-5M calls per month	$0.006
5M-10M calls per month	$0.005
Adaptive Audio per Call Fees	
250K-1M calls per month	$0.007
1M-5M calls per month	$0.006
5M-10M calls per month	$0.005
Business Intelligence Gateway Monthly Fee[1]	
Monthly subscription, up to 5 users	$2,500

Notes:
1) Included at no additional charge with purchase of Adaptive Recall or Adaptive Audio

Adaptive Fraud	
Knowledge Based Authentication (KBA)	
Per call fee	$0.50
Red Flags monthly fee[1]	
0-1M calls per month	$10,000
1M-5M calls per month	$25,000
> 5M calls per month	$50,000

Notes:
1) Based on total inbound calls per month

Two-way Text Messaging	
Per message fees	
Mobile terminated	$0.025
Mobile originated	$0.025
Hosting/leasing fees	
Random dedicated short code	$1,250
Vanity dedicated short code	$1,875
Email On-demand	
Per message fee	$0.02

Technical Proposal

In response to:

RFP CH16012 – Cloud Solutions

Submitted to:

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

Submitted by:

Michael Southworth, CEO
Contact Solutions, LLC
11950 Democracy Drive, Suite 250
Reston, VA 20190
Phone: (571) 385-1283
Fax: (703) 480-1676
msouthworth@contactsolutions.com

March 10, 2016

Contact Solutions
A VERINT Company
11950 Democracy Drive • Suite 250 • Reston, VA 20190 • P 703.480.1620 • F 703.480.1676

5.2 Cover Letter

March 10, 2016

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

Re: RFP CH16012 – Cloud Solutions

Dear Mr. Hughes and members of the proposal evaluation committee:

Contact Solutions, a Verint company, is pleased to offer this proposal in response to your RFP for cloud solutions. We are the premier provider of cloud-based Interactive Voice Response (IVR) solutions to government agencies in the United States. We help governments at all levels automate a portion of their phone-based interactions with citizens in a way that improves customer service and satisfaction while reducing costs. We feel that Participating Entities will find this a valuable offering and we pledge to market this Master Contract throughout the NASPO membership to help them improve the ways they interact with their constituents.

In compliance with RFP Section 5.2, we provide the following statements:

5.2.1 Contact Solutions understands that it may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

5.2.2 The following firms and/or staff were responsible for writing the proposal:

- Michael Southworth, Contact Solutions, Chief Executive Officer
- Vete Clements, Contact Solutions, Chief Operating Officer
- Tim Grimes, Contact Solutions, Senior Vice President, Sales
- Dan Raup, Contact Solutions, Director of Market Development
- Jeff Ormsbee, Contact Solutions, Principal Security Engineer
- Jennifer Poppell, Contact Solutions, Senior Manager, Sales Operations
- Andrea Katsivelis, Contact Solutions, Product Marketing Manager
- Kathleen Fischer, Vencore, 3PAO Operations and Technical Manager
- Viswa Kumar, Vencore, Director, 3PAO and Quality Management
- Jeff Lowe, Editorial Services Consultant

5.2.3 Contact Solutions is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

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

5.2.5 Contact Solutions proposes to provide the following service models and deployment models in this contract:

- Service model – SaaS
  - Other – Interactive Voice Response
- Deployment model - private cloud

5.2.6 Contact Solutions is capable of storing and securing the following data risk categories: Low Risk Data and Moderate Risk Data

NOTE: We have completed Attachment H and include it directly following the Table of Figures.

Thank you for this opportunity.

Sincerely,

Michael Southworth, CEO
Phone: (571) 385-1283
Fax: (703) 480-1676
msouthworth@contactsolutions.com

Table of Contents

Table of Figures

Appendices

The following documents have been uploaded as separate files. Where appropriate, we refer to them in the body of this proposal.

5.1 Signature Page

5.3 Acknowledgement of Amendments

Exhibit 1 to Attachment B_CAIQ

Exhibit 2 to Attachment B_CCM

Contact Solutions Sample Service Level Addendum

Contact Solutions Issued Financials 2013-2014-CONFIDENTIAL

Contact Solutions SSAE 16 SOC1 Audit Report Calendar Year 2014

Contact Solutions SSAE 16 SOC2 Audit Report Calendar Year 2014

Contact Solutions Standard Security Operations, Policies, and Procedures

Contact Solutions Janet Mero Resume-CONFIDENTIAL

Contact Solutions Sample Project Plan

Contact Solutions Sample Performance Report

Contact Solutions IVR SaaS - CSA STAR Self-Assessment

Contact Solutions IVR SaaS - CSA STAR Continuous Monitoring

Contact Solutions Disaster Recovery and Business Continuity Plan

Contact Solutions Claim of Business Confidentiality

Attachment H – Identification of Service Models Matrix

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

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
SaaS	Yes	Yes	Not at this time	Contact Solutions intends to provide Software as a Service (SaaS) via private cloud with the following subcategories. • Other – Interactive Voice Response
IaaS	(Bundled with SaaS)	(Bundled with SaaS)	N/A	
PaaS	(Bundled with SaaS)	(Bundled with SaaS)	N/A	

Contact Solutions uses the following guidance extracted from *NIST Special Publication 800-60 Volume II, Revision 1, Guide for Mapping Types of Information and Information System to Security Categories.*

Type-based Impacts for Federal Information and Information Systems Security Categorization of Management and Support Information			
	Confidentiality	**Integrity**	**Availability**
Controls and Oversight			
Corrective Action (Policy/Regulation)	Low	Low	Low
Program Evaluation	Low	Low	Low
Program Monitoring	Low	Low	Low
Regulatory Development			
Policy and Guidance Development	Low	Low	Low
Public Comment Tracking	Low	Low	Low
Regulatory Creation	Low	Low	Low
Rule Publication	Low	Low	Low
Planning and Budgeting			
Budget Formulation	Low	Low	Low
Capital Planning	Low	Low	Low
Enterprise Architecture	Low	Low	Low
Strategic Planning	Low	Low	Low
Budget Execution	Low	Low	Low
Workforce Planning	Low	Low	Low
Management Improvement	Low	Low	Low
Budgeting & Performance Integration	Low	Low	Low
Tax and Fiscal Policy	Low	Low	Low

Type-based Impacts for Federal Information and Information Systems Security Categorization of Management and Support Information			
	Confidentiality	**Integrity**	**Availability**
Internal Risk Management and Mitigation			
Contingency Planning	Moderate	Moderate	Moderate
Continuity of Operations	Moderate	Moderate	Moderate
Recovery	Low	Low	Low
Revenue Collection			
Debt Collection	Moderate	Low	Low
User Fee Collection	Low	Low	Moderate
Federal Asset Sales	Low	Moderate	Low
Public Affairs			
Customer Services	Low	Low	Low
Official Information Dissemination	Low	Low	Low
Product Outreach	Low	Low	Low
Public Relations	Low	Low	Low
Legislative Relations			
Legislation Tracking	Low	Low	Low
Legislation Testimony	Low	Low	Low
Proposal Development	Moderate	Low	Low
Congressional Liaison Operations	Moderate	Low	Low
General Government			
Central Fiscal Operations4	Moderate	Low	Low
Legislative Functions	Low	Low	Low
Executive Functions5	Low	Low	Low
Central Property Management	Low	Low	Low
Central Personnel Management	Low	Low	Low
Taxation Management	Moderate	Low	Low
Central Records and Statistics Management	Moderate	Low	Low
Income Information	Moderate	Moderate	Moderate
Personal Identity and Authentication	Moderate	Moderate	Moderate
Entitlement Event Information	Moderate	Moderate	Moderate
Representative Payee Information	Moderate	Moderate	Moderate
General Information	Low	Low	Low

5.3 Acknowledgement of Amendments

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the final RFP document posted on February 3, 2016, the amended Attachment A, and the answers to the questions posted by offerors on Bidsync.

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

Contact Solutions, LLC
Offeror

Michael Lundhund
Representative Signature CEO

5.4 Executive Summary

Who we are

Contact Solutions, a Verint company[1] based in Reston, Virginia, has been a trusted provider of hosted, cloud-based IVR solutions for many state programs with presence in 43 states - delivering 56 programs for Child Support, CHIP, Child Care, Child Protective Services, Corrections, Eligibility, DMV, HIX, MMIS, Payroll, Parking, Surcharge, TANF, Ticketing, Treasury, UI and WIC. Our domain and thought leadership in cloud-based customer self-service and contact center infrastructure is unmatched and is gleaned from our vast experience with government programs.

- We deliver over 120 million calls per month for our clients.
- We support a major Federal entitlement program with over 4M active cardholders and monthly loads in excess of $2.5B with a growth forecast that predicts usage to double in the next two years.
- Some of our largest projects include providing self-service access to electronic benefits transfer recipients in California, Florida, Texas, Michigan, and Illinois.

Our experience with these and other government programs means we can provide fast, reliable support for any Purchasing Entity that needs to provide its constituents with effective self-service functions.

Why you should choose Contact Solutions

1. Our **experience with a large diversity of government programs** will empower Purchasing Entities to achieve savings and efficiencies in virtually any public service function involving phone-based citizen contacts.
2. Contact Solutions is the **premier provider of such IVR solutions** to the kinds of government agencies that are represented by the NASPO community.
3. We have both the credentials and proven track record to ensure **complete data security** for Purchasing Entities and their constituencies.
4. Our carrier grade IVR service is a true "cloud" solution that will service the NASPO community with geographically dispersed call handling, redundancy and failover capabilities that have been proven to provide **unmatched business continuity for 10 years**.
5. A track record of **self-service innovation** (to include fraud, personalization and mobility) and actionable intelligence that fully leverages the analytics we capture and that are associated with the over 1B transactions processed annually on our platform.

[1] Contact Solutions was acquired by Verint on February 22, 2016.

6. Our thought leadership in the IVR industry is translated into **contact center best practices** that keep Purchasing Entities in line with constituent expectations and the market.
7. We make it **very easy for Purchasing Entities to implement and operate** our IVR solution without having to add to their own technical infrastructure and associated maintenance effort.
8. We will **aggressively promote** the Contract through the NASPO community.
9. Contact Solutions offers a **Contract Manager with over 25 years of Federal and State government experience** delivering and managing technology solutions. She has been responsible for managing million dollar implementations and contracts across 39 states.

The solution we propose

Functionality: Using our private, distributed, cloud infrastructure and our expertise in automating call interactions between citizens and government agencies, we will develop and host systems to enable citizen self-service for interactions such as:

- address verification
- appointment reminders
- applications status
- authentication
- beneficiary information
- child protection reports
- child support disbursement
- EBT, assistance programs
- eligibility, enrollment
- fee/ticket payment
- help desk
- information alerts & reminders
- life change updates
- password reset
- probationer reporting
- provider/broker/payer support
- satisfaction surveys
- registration/enrollment/activation

Hosting infrastructure: Our infrastructure ensures business continuity and system redundancy for all the IVR applications we host, with **zero platform downtime in the past 10 years**. Call-handling load is automatically and dynamically balanced across three geographically dispersed, continuously linked, yet independently operable data centers. This architecture produces a **massively scalable, peak neutral**, hosted IVR within a cloud platform that is **SSAE-16 certified and PCI and HIPAA compliant.**

Data security: Every government program we support with our IVR requires us to **handle confidential and otherwise sensitive data**. In collaboration with government agencies across the nation, we have developed architectural, logical, and operational methods to safeguard this information in ways that meet all applicable standards. We manage access to the IVR platforms using a combination of industry standard firewall technology, key fob RSA security tokens, VPNs and account name/password user login management. We employ effective approaches for:

- Penetration testing and vulnerability scanning
- Intrusion detection system (IDS)
- Network firewalls
- VPN platform access

- Password management and control
- Virus detection and protection
- Network device security log management
- Client site-to-site network integration

How our offering fits this solicitation

Virtually all Participating Entities eligible to use this contract conduct a substantial level of interaction with the public via the telephone. In many cases, they rely on the contact center as the main interface with constituents who need information, support, and services – with the IVR as the first contact point citizens have. A poor or difficult experience can cause a longer, more costly live representative interaction, operational impacts in how citizens are served and supported, and a risk of negative public opinion over time.

Properly automating a portion of those calls can vastly improve the efficiency and effectiveness of these programs, while saving money and giving citizens a 24/7 telephone self-service channel to access services and solve their needs in a faster, more satisfying manner. Our IVR services also give Purchasing Entities the business intelligence needed to continuously improve services and adapt to changing circumstances, while better serving their constituents.

Our adaptive IVR solution is a **reliable, secure, cloud-based, Software-as-a-Service (SaaS)** solution that meets all of the solicitation's minimum requirements and other needs and standards. Using our private cloud, Purchasing Entities will be able to **easily implement and use world-class IVR functionality and expertise affordably** and without having to acquire and maintain any new technology of their own.

Our approach to marketing

Contact Solutions will **promote this contract as a go-to source for government IVR solutions among the NASPO community.** We will post the information about the contract on our website. We will also provide Twitter and LinkedIn feeds from our Contact Solutions accounts as well as providing them for our employees to post on their own accounts. Links to the NASPO website, to the Master Agreement and to the States with Participating Addendums will also be included. We will:

- Develop NASPO customer information and promotional materials
- Develop and promote NASPO website page, including links to MA, PAs
- Use datasheets, blog posts, and case studies to educate and inform buyers
- Engage with Lead State, NASPO, Cooperative Purchasing Organization (CPO)
- Participate in various state marketing activities and events
- Utilize social media, datasheets, table top displays, emails, giveaways
- Leverage relationships for references, recommendations, and referrals

5. Mandatory Minimums

Contact Solutions meets or exceeds all of the mandatory minimums in this RFP.

Please note that in accordance with RFP instructions we have included the other major subsections of RFP Section 5 as follows:

- 5.1 Signature Page – separate uploaded file
- 5.2 Cover Letter – above in this document
- 5.3 Acknowledgement of Amendments – above in this document
- 5.4 Executive Summary – above in this document

5.5 General Requirements

5.5.1 Usage Report Administrator

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

Contact Solutions complies with this requirement. We will provide a Usage Report Administrator as requested.

We provide similar administrative reporting functions to other government clients and thus have the personnel, experience, and tools to do so for this contract.

5.5.2 Cooperate with NASPO ValuePoint and SciQuest

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

Contact Solutions complies with this requirement. We agree to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

5.5.3 CSA Star Registry Self-Assessment

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

Contact Solutions has completed the CSA STAR Attestation, included as a separate file entitled Contact Solutions IVR SaaS - CSA STAR Self-Assessment.

Contact Solutions has completed The Consensus Assessments Initiative Questionnaire (CAIQ), included as a separate file entitled Exhibit 1 to Attachment B_CAIQ.

Contact Solutions has completed the report documenting compliance with Cloud Controls Matrix (CCM), included as a separate file entitled Exhibit 2 to Attachment B_CCM.Contract Solutions has completed the CAIQ and CCM with data collected as of February 2016 and certifies that the information gathered is accurate and representative of the security posture of the information system. These documents were assessed and completed by a FedRAMP 3PAO (Third-party Assessment Organization), accredited by A2LA to perform Cloud Security assessments pursuant to FedRAMP. The 3PAO is also a certified FITSP, Auditor and Trainer by Federal IT Security Institute (FITSI), and Certified Expert in Cloud Security (CECS). The third-party annual assessment for PCI and SSAE 16 was successfully completed in January - February 2016, and final reports are pending.

5.5.4 Service Level Agreement

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.

Contact Solutions will work with individual Purchasing Entities to define agreed upon SLAs. In general, Contact Solutions adheres to a 99.999% service level.

We have included a sample Service Level Agreement as a separate file entitled Contact Solutions Sample Service Level Addendum.

NOTE: The RFP does not include a section 5.6. Our proposal matches the RFP in omitting this section from our numbering.

5.7 Recertification of Mandatory Minimums and Technical Specifications

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

Contact Solutions complies with this requirement. We agree that if awarded a contract under the RFP, we will annually certify to the Lead State that we still meet or exceed the technical capabilities discussed in our proposal. Contact Solutions will make available external third-party audit reports and self-attestations to confirm

the security posture of the information systems provided under this contract vehicle.

Contact Solutions publishes a Service Organization Controls 2 (SOC 2), Type II report that is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls (industry best practices) relevant to security, availability, processing integrity, confidentiality, and privacy applicable to cloud service organizations such as Contact Solutions. The SOC 2 Controls align with many industry standards including NIST, CSA, FedRAMP, and PCI as demonstrated by the Cloud Controls Matrix (CCM), which provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance

The Contact Solutions SOC 2 documents compliance of design and operating effectiveness of controls that meets the criteria for the security principles set forth in the AICPA's Trust Services Principles. The SOC 2 report provides additional transparency into Contact Solutions security based on a pre-defined industry standard of leading practices and further demonstrates Contact Solutions' commitment to protecting the client and citizens' data.

6. Business Information

6.1 Business Profile

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

Contact Solutions has provided a response to this requirement in the following section: Confidential, Protected, or Proprietary Information, 6.1 Business Profile on page 101. Click the cross reference to jump to that section.

6.2 Scope of Experience

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

Contact Solutions has provided a response to this requirement in the following section: Confidential, Protected, or Proprietary Information, 6.2 Scope of Experience on page 101. Click the cross reference to jump to that section.

6.3 Financials

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

Contact Solutions has provided a response to this requirement in the following section: Confidential, Protected, or Proprietary Information, 6.3 Financials on page 104. Click the cross reference to jump to that section.

6.4 General Information

6.4.1. Acceptance of solution in cloud marketplace

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

Contact Solutions has been a trusted provider of hosted, cloud-based IVR solutions for many state programs with presence in 43 states - delivering 56 programs for Child Support, CHIP, Child Care, Child Protective Services, Corrections, Eligibility, DMV, HIX, MMIS, Payroll, Parking, Surcharge, TANF, Ticketing, Treasury, UI and WIC. Our domain and thought leadership in cloud-based customer self-service and contact center infrastructure is unmatched and is gleaned from our vast experience with government programs.

We have been recognized by Frost and Sullivan as **one of the top 5 market share providers in the North America Hosted Contact Center Market**. The company's expertise, reputation, and offerings have been recognized by industry analysts and clients alike.

Figure 1: Contact Solutions Leadership in the IVR Market

Government departments are typically faced with the dilemma of limited resources and growing, ever-more-demanding constituencies. Within that context, constituent care must be sustainable in cost and quality over the long term. Agencies can't afford to choose between inconsistent service and budget overruns, and have aligned technology with constituent customer experience to provide program support that combines performance with affordability.

Cloud-based technology is one of the leading trends in IT today. Cloud constituent engagement tools generally provide improved capabilities of an on premise system without the headaches and expense of installation and maintenance. The Federal Government's Cloud First policy directs agencies to take full advantage of cloud computing to maximize capacity utilization, improve IT flexibility and responsiveness, and minimize costs. Purchasing Entities can achieve similar benefits by adopting a cloud strategy for IVR and digital engagement.

- Delivers easier to manage rollout and ongoing administration

- Supports security and compliance measures
- Ensures high reliability by leveraging redundant infrastructure in case of an interruption
- Provides seamless expansion capability to meet additional constituent demand

State agencies are looking at trends in cloud solutions, vendor management and consolidation, fraud prevention and management across all constituent and state worker interaction points, and automated self-service solutions that improve constituent satisfaction while easing the burden on workers and optimizing scarce resources. Agencies are also looking for sustainable solutions that can support:

- Agility to keep pace with changes in constituent needs, technology, and evolving policies and programs, with digital and mobile options, better personalization, and dynamic IVR that allows individuals to self-serve to solve their issues in a faster, flexible way
- Ease of use and convenience for each individual, regardless of preferences, which saves time and resources for both the constituents and the agency
- Cost-effectiveness to get the most from budget dollars, by streamlining solutions and engaging vendors who can manage the burden of compliance, technology, and care in the most efficient ways possible
- Consistently high quality, as measured by satisfaction ratings, customer experience, and response times – followed by reduced time required by state workers for support
- Multi-layered fraud prevention tools that are integrated within the customer care solutions, to prevent fraud and nuisance callers in IVR - before they create havoc in the contact center - while improving overall authentication processes and customer experience
- Adoption of Integrated Eligibility Systems to streamline constituent benefit management processes, to consolidate communication channels and improve access to information and service, and a holistic view of constituent and agency engagement

Contact Solutions cloud-based Software-as-a-Service (SaaS) solutions provide these technologies and capabilities consistently. We have earned an excellent reputation among our government clients for our professionalism in delivering these solutions to meet the needs of agencies and citizens alike. This has resulted in a 100% client retention rate on our direct contracts.

Government agencies everywhere are increasingly realizing that IVR self-service can vastly improve the reach, accessibility, and usability of their public service programs. IVR also empowers them to better allocate limited budgets to meet increasing expectations of their constituents. Contact Solutions is the market leader in helping government agencies meet these difficult challenges.

Citizens who use government programs need the ability to acquire and deliver information in the manner, mode, media, and format most convenient and accessible to them. The device will vary based on the individual's preference. As a long-time leader in providing solutions to the government sector, Contact Solutions has developed methods to accommodate all of these preferences in a seamless, full-spectrum communications environment. Such comprehensive access to information and services improves the public's satisfaction with government programs.

Contact Solutions' spike-neutral, highly scalable, reliable, cloud-based IVR creates effortless customer care for state constituents through highly personalized experiences. Each call is tailored to the individual citizen based on previous caller activity and session activity (e.g. speed of response, level of user difficulty) to drive preference for easier self-service, with prompt transition to a representative when needed, in a highly secure platform, using proprietary business intelligence, and call processing software. Our cloud platform is SSAE-16 certified and PCI and HIPAA compliant, and has delivered zero downtime in the past 10 years, processing in excess of 1 billion calls per year.

Our solutions rely on business intelligence at the core to improve and personalize Customer Experience (CX) and drive better operational performance, while having the ability to manage the risk of fraud. Contact Solutions can help Purchasing Entities offer effortless care – in both self-service and live agent interactions – at a sustainable cost while adapting quickly to rapidly changing constituent demands.

6.4.2 Auditing Capabilities

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

Contact Solutions employs rigorous, documented, implemented, and monitored security standards, which have been and continue to be reviewed as part of a Level 2 SSAE-16 audit. We are SSAE-16 certified. Contact Solutions' SOC1 and SOC2 audit reports are included as separate files entitled Contact Solutions SSAE 16 SOC1 Audit Report Calendar Year 2014 and Contact Solutions SSAE 16 SOC2 Audit Report Calendar Year 2014. Contact Solutions will make available external third-party audit reports and self-attestations to confirm the security posture of the information systems provided under this contract vehicle.

6.5 Billing and Pricing Practices

6.5.1 General description, transparency, easy to understand

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

We understand that in today's world flexibility plays an important role in managing the billing process of our customers. Depending on the Purchasing Entity's needs and contractual requirements, bills will be broken out by a line item description, quantity, unit price and amount. All invoices are sent via email for a quick and convenient delivery. We accept payment by ACH or check, whichever is more convenient for the Purchasing Entity. We can combine multiple applications under the same bill, thus providing a consolidated view in one easy-to-read format. Our reporting capabilities can show daily, weekly or monthly volume in an easy-to-read Excel format. Should a Purchasing Entity choose consolidated billing, we can easily accommodate this, providing:

- Fewer invoices and less paperwork, saving time and money,
- Better money management because work is billed routinely and accurately,
- Better review and control of budgets,
- No additional cost for customization of billing.

Although we strive to ensure accuracy the first time around, if a problem should occur, Contact Solutions will resolve all invoice issues as quickly as possible. On each invoice the Purchasing Entity will see a direct contact number and email who will be more than happy to assist should any discrepancy arise. Pricing is established through the MSA and/or SOW in a table format with easy to read rates. All rates, maintenance and one-time charges are displayed through a billing attachment, providing a quick and easy way of understanding the charges.

6.5.2 Typical cost impacts

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

Unlike premise-based models, Contact Solutions' hosted cloud approach requires no up-front investment in equipment or software. Instead, our model relies on an initial application delivery fee and per-transaction fees that allow organizations to pay for only those resources and services they actually use.

6.5.3 NIST compliance

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

Contact Solutions' Interactive Voice Response (IVR) product offers a Software-as-a-Service (SaaS) solution via private cloud, which is fully compliant with NIST Special Publication 800-145, The NIST Definition of Cloud Computing.

The IVR capability provided to the client uses Contact Solutions' applications that run on a cloud infrastructure. The client does not manage or control the underlying

cloud infrastructure including network, servers, operating systems, or storage. Individual application capabilities, limited to user-specific application configuration settings, are accessible from various client devices through a web browser. The IVR SaaS can be interfaced to connect directly to the clients' information systems to drive response, collect data, or support other client requirements.

The IVR product is deployed as a private cloud. The cloud infrastructure is provisioned for exclusive use of each client. It is managed and operated by Contact Solutions, and it exists off premise in three certified data centers, geographically disbursed in the continental United States.

The IVR solution has broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., telephones, mobile phones, voice over IP, tablets, laptops, and workstations). Contact Solutions' computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

The IVR capabilities can be elastically provisioned and released, automatically, to scale rapidly outward and inward commensurate with demand. The Contact Solutions IVR product automatically controls and optimizes resource use by leveraging a metering capability. Information system resource usage can be monitored, controlled, and reported, providing transparency for both the provider and client of the utilized service.

6.6 Scope and variety of cloud solutions

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

Contact Solutions offers Interactive Voice Response (IVR) with associated business intelligence and customer relationship management functions in the SaaS, private cloud model.

Contact Solutions has been a trusted provider of hosted, cloud-based IVR solutions for many state programs with presence in 43 states. Our domain and thought leadership in cloud-based customer self-service and contact center infrastructure is unmatched and is gleaned from our vast experience with government programs. With a clear understanding of how to address constituent needs, the areas of distinction that separate Contact Solutions are our key platform capabilities of:

- Massively scalable, peak neutral, hosted IVR with a rich set of Web, 1-way and 2-way SMS, email, surveys, fax, outbound, and CTI solutions
- IVR systems deployed in a distributed network with geographically diverse hosting facilities in Virginia, Texas and California - IVR equipment and all

supporting services and telecommunications infrastructure are redundant in each location

- Business intelligence that synthesizes data and applies analytics to personalization, CX, continuous improvement focus, fraud management
- Multi-layered, IVR Fraud Management to predict, detect, and stop fraudulent activity through automated processes within the IVR
- Dynamic IVR with patented personalization that delivers in-depth reporting insights, dynamic, preference- and behavior-based personalization, driven by real-time analytics
- Virtually any language can be supported in speech, text-to-speech or touch tone
- Lower Costs

IVR – Automated Self-Service

Our IVR service is a reliable, secure, cloud-based, Software-as-a-Service (SaaS) solution that meets all of the solicitation's minimum requirements and other needs and standards. Using our private cloud, Purchasing Entities will be able to easily implement and use world-class IVR functionality and expertise affordably and without having to acquire and maintain any new technology of their own.

Rich self-service features:

- Call routing
- Transaction processing
- Surveys
- Outbound notifications
- Identity authentication/verifications
- Pay-by-phone
- Call deferral/call back
- 1-way and 2-way SMS
- Outbound email/fax
- Secured voice messaging
- Multi-lingual

Contact Solutions' IVR leverages a robust business intelligence framework to create highly personalized experiences. Our hosted self-service delivers superior care at a sustainable cost and adapts quickly to rapidly changing customer demand. It creates a flexible, highly reliable, and scalable environment and removes operational and technical burdens that legacy and premise systems struggle to reduce. And we guarantee our results.

- Massively scalable to support call volume increases and peaks
- Highly redundant service delivery platform, with zero downtime since 2004
- Seamless integration with CRM and other back-end systems
- Fully secure - SSAE-16 certified and PCI and HIPAA compliant
- Billions of transactions across diverse commercial and government customers

Sample IVR applications:

Presence	56 State, Local and Federal Programs in 43 States		
Programs We Support	Human Services • Child Support/SDU • Child Care • Child Protective Services • Eligibility and Enrollment • Integrated Eligibility Systems Provider • SNAP • TANF • WIC	Other Programs • CHIP • Corrections, probation • DMV, Courts • HIX • MMIS • Parking • Payroll • Surcharge • Ticketing • Treasury • UI	
Typical Interactions	• Address, dependent verifications • Appointments • Application Status • Authentication • Beneficiary information, inquiries • Bill processing • Case worker requests • Child Support disbursement, deposit • Claims/cases • EBT, assistance program (deposit, balance, retailer) • Eligibility, enrollment	• Fee/ticket payments/collections • Help desk • Life change updates, status • Password reset • Plan availability • Provider searches • Provider, broker, payer support • Registration/enrollment/ activation • Reminders, information, alerts • Requests for information • Satisfaction survey	
Application Types	• Authentication • Call deferral/call back • Fax, Email, Web • IVR router/transactional • Outbound notifications	• Pay-by-Phone • Pay-by-Web • Ready Response • Survey	• Text/SMS, 1-way and 2-way • Verifications
Key Metrics	• Over 120 million calls/month • Over 95% automation rate • SNAP - 97% average call containment (both client and retailer combined) • TANF - 98.5% average call containment (client only) • Over 80% MMIS automation rate		

Proactive Outbound Notifications

Proactive outbound notifications can keep citizens informed of updates and status changes and reduce the burden on the agency and the citizen. Providing such proactive messaging will enable citizens to track status more easily and enable government employees to focus on more complex tasks. For example, we provide outbound pending deposit notifications for a reloadable card program that has resulted in 11.4% fewer calls, faster resolution rates, and decreased need for call back.

Contact Solutions Optimization Portal

In addition, every Contact Solutions IVR is built such that it can be securely administered through a web portal management tool. Contact Solutions Optimization Portal employs role-based controls so viewing and changing system behavior can be restricted to specific logins and passwords.

The Optimization Portal provides a tool to manage application configuration parameters and affect features and functionality in real-time; including creating and uploading temporary messages at strategic points in the call flow. This approach allows Purchasing Entities to add temporary messages when important events occur (i.e. program changes, call center closings, natural disasters, etc.).

For many IVR providers, the process of recording, testing and deploying a message or call flow change can take hours if not days. Often, the potential impact of the information provided in a temporary message is critical to constituents. Our web-based tool allows Purchasing Entities to record and upload messages in fewer than five minutes, providing the ability to customize messages in near real time.

The IVR Optimization Portal also allows comprehensive management changes which are affected in real-time. For example, on command an outbound campaign can be completely turned off, or the flow of calls can be throttled to variable levels to meet changing staffing levels at the call-centers for bridged calls, etc.

Reporting

Contact Solutions offers a wide array of reporting options for Purchasing Entities to utilize as part of the out of the box reporting solution. Samples of available reports are: call flow exit points, transfer status, inbound calls by DNIS, call volumes, and automation rates. There are various other low level details about each call such as performance of host integrations that are available out of the box as well.

Reports can be pulled delivering up-to-the-minute information about caller activity and system performance. Reports can take the form of traditional tabular data or graphic displays. Information can be delivered on a regular basis (daily, weekly, monthly, etc.) via email or in near real-time via a web portal.

Contact Solutions converges data from across customer service channels, eliminating silos of information, revealing greater visibility to self-service intelligence across the constituent interaction and engagement process. By collecting interaction data across our solutions, Contact Solutions empowers Purchasing Entities to better understand constituent behavior and preferences.

Business Intelligence

Constituent contact center interactions, especially self-service transactions, generate massive amounts of data that can help meet constituent needs and navigate the risks of fraud—but only if access to the data is easily and effectively delivered to meet a Purchasing Entity's flexible needs. Contact Solutions' Business Intelligence (BI) Gateway is a cloud-based analytics tool that offers greater visibility to customer self-service intelligence across interactions, helping Purchasing Entities

more effectively and accurately monitor performance, assess and improve CX, and identify cost savings opportunities.

Our solution enables a view and understanding of constituent activity, preferences, and program metrics within a specific program, and across multiple programs, to help Purchasing Entities better meet the needs of their constituents.

- Precise reporting and analytics
- Complements existing data tools to better serve your customers
- Flexible, dimensional data that can be "sliced and diced"
- Ability to create your own reports
- Convenient access
- Deeper understanding of constituent intent, behavior, and experience

Our customers benefit from instant access and insights into a Dashboard and Reports views of constituent interactions at a high-level view with drill-down options. These actionable, easy-to-read standard dashboards are available on-demand and provide instant access to meaningful customer success data to improve your interaction strategies.

Integration with Existing Systems

Based on experience delivering hundreds of self-service solutions for government clients, Contact Solutions recognizes that stable, secure and resilient connectivity to host systems and networks is critical to providing the highest quality self-service.

Contact Solutions has experience in the following key areas:

- Seamlessly integrating with the full range of systems that may be employed by the Purchasing Entity; from legacy mainframe systems to the latest RESTful web services.
- Designing host integrations that meet the needs of government programs and their constituents.
- Developing host integrations that are flexible, sustainable and efficient.
- Continuous monitoring of host connections to ensure maximum uptime.

Computer Telephony Integration (CTI):

CTI allows constituent data collected from the IVR to be used as input data to query databases with constituent information and populate that data instantaneously in the customer service representative screen. The net effect is the agent already has the required screen on his/her terminal before speaking with the constituent.

When the call reaches the contact center, the Purchasing Entity's contact center platform requests the data associated with call. Once the data is passed from Contact Solutions to the contact center, the Purchasing Entity's contact center agent software presents the CTI data to the agent.

ID Verification / Fraud Prevention

Contact Solutions provides a comprehensive approach to identify, prevent and report on potential fraudulent activity in the IVR channel. We utilize best practices from the Network Branded Prepaid Card Association, and those we have built over time, to reduce the threat of fraud including the use of multi-layer authentication (which may include optional 3rd party verification), account access restriction after too many unsuccessful authentication attempts, and outbound notifications of transactions to help constituents detect when their account may have been compromised.

We can authenticate users on multiple factors and even offer alternate authentication methods should the constituent not know the answer to the primary authentication method. This feature functionality can be expanded to include speech recognition for unique alpha-numeric and phrase base identifiers.

Contact Solutions' Adaptive Fraud Prevention solution is based on an IVR specific threat matrix developed with industry experts, and validated through data mining. Through partnerships with our technology partners, the solution delivers real-time fraud prevention in the IVR to take security risks out of state contact center operations.

With Adaptive Fraud Prevention, Purchasing Entities can:

- Discreetly detect and stop probing activity in the IVR
- Provide heightened authentication for high risk automated transactions
- Reduce fraud losses and prevent account takeovers
- Adapt and respond to changes in fraud patterns

6.7 Best practices

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

Contact Solutions employs rigorous, documented, implemented, and monitored security standards, which have been and continue to be reviewed as part of a Level 2 SSAE-16 audit and PCI compliance review. We are SSAE-16 certified and PCI and HIPAA compliant.

Access Management: We manage access to the IVR platforms with a combination of industry standard firewall technology, key fob RSA security tokens, VPNs and account name/password user login controls.

Data Transmission and Encryption: Contact Solutions has multiple methods to transport data securely:

- Encrypted VPN tunnels

- Private Data Circuit
- Secure HTTP transmission using certificates
    - Latest SSL encryption required for transmission
    - HTTPS is required in the URL
- Secure FTP

Data Storage: Contact Solutions stores non-sensitive client related data locally within the platform database infrastructure. Our platform architecture allows sensitive data to be segmented on physically separate database servers if required.

Additionally, Contact Solutions mandates data masking techniques to ensure that data (i.e. account numbers, SSN, etc.) is stored securely and without manual inspection. Contact Solutions allows for the storage of the first 6 digits or the last 4 digits of sensitive card data, but not full Personal Account Number (PAN) or credit card number. Storage of both within the same application is prohibited.

Contact Solutions prohibits the storage of credit/debit card track data, CVV2 and PIN codes.

Data Encryption Key Management Policy: Contact Solutions uses a two-tiered encryption architecture to encrypt sensitive customer information, including a symmetric AES_256 encryption key and stored in a separate database.

The AES_256 encryption key is further encrypted using a certificate generated with the database master encryption key (key-encrypting key). Full password to the AES_256 encryption key is not known by any one individual and is stored on the database server in an unreadable format. All backup encryption keys are centrally stored on a secure management server.

We have included our security policies as a separate file entitled Contact Solutions Standard Security Operations, Policies, and Procedures.

7. Organization Profile

7.1 Contract Manager

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

Contact Solutions has provided a response to this requirement in the following section: Confidential, Protected, or Proprietary Information, 7.1 Contract Manager on page 105. Click this cross reference to jump to that section.

7.1.1 Contract Manager contact information, work hours

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

Contact Solutions has provided a response to this requirement in the following section: Confidential, Protected, or Proprietary Information, 7.1.1 Contract Manager contact information, work hours on page 105. Click this cross reference to jump to that section.

7.1.2 Contract Manager experience, resume

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

Contact Solutions has provided a response to this requirement in the following section: Confidential, Protected, or Proprietary Information, 7.1.2 Contract Manager experience, resume on page 105. Click this cross reference to jump to that section.

7.1.3 Contract Manager roles and responsibilities

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

Our Contract Manager will:

- Draft, evaluate, negotiate and execute all contracts associated with the Master Agreement including NDAs and specific proposed terms and conditions.

- Be the point of contact for NASPO and Participating Entity staff on contractual matters, ensuring timely review and approval/reconciliation of variations.
- On all contracts, provide redlined recommendations and often negotiate directly with NASPO and Participating Entity staff until consensus has been reached.
- Maintain contractual records and documentation such as receipt and control of all contract correspondence, NASPO and Participating Entity contact information sheets, contractual changes, status reports and other documents for all projects.
- As needed, provide guidance on contract matters to project managers or other operational staff, including training to new project managers and other employees in contracting practices and procedures.
- Develop and implement procedures for contract management in compliance with company policy, and contribute to or influence company policies.
- Monitor employees' compliance with procedures. Identify areas of concern.
- Work with Risk Management Department / Finance to coordinate contractual insurance requirements.
- Work with Security Officer to comply with information security requirements.
- Work with Finance to adhere to finance and risk requirements such as revenue recognition, pricing and discounting policies. May include 'financial engineering' and understanding/evaluating economic impact of terms and term options.
- Support Product Management / Marketing to ensure company products and services are offered with appropriate, competitive terms and conditions.
- Monitor competitive terms. Monitor NASPO and Participating Entity satisfaction with our terms and conditions and contracting practices. Recommend changes.
- Ensure that signed contracts are communicated to all relevant parties to provide contract visibility and awareness, interpretation to support implementation.
- Handle ongoing issue and change management.
- Monitor transaction compliance (milestones, deliverables, invoicing. etc.) and oversee SLA compliance.
- Ensure contract close-out, extension or renewal.

8. Technical Response

8.1 Technical Requirements

8.1.1 Identify cloud service and deployment models

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

Contact Solutions intends to provide Software as a Service (SaaS) via private cloud.

8.1.2 Meeting NIST essential characteristics

8.1.2.1 On-demand self-service

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

The Contact Solutions Optimization Portal provides a web-based tool to manage application configuration parameters and affect features and functionality in real-time. Configurable items such as Temporary Messaging, Call-Center Routing, Outbound Call Frequency, and other parameters required to be changeable in a moment's notice are managed right from a Web browser. Access to the features is role-based and different access for viewing and changing system behavior can be restricted to specific login-IDs.

8.1.2.2 Broad Network Access

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

The IVR solution has broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., telephones, mobile phones, voice over IP, tablets, laptops, and workstations).

8.1.2.3 Resource Pooling

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

Contact Solutions' computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

8.1.2.4 Rapid Elasticity

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

The IVR capabilities can be elastically provisioned and released, automatically, to scale rapidly outward and inward commensurate with demand. Elastic capacity ensures all calls get through – even during the busiest calling periods or when unplanned events occur. Our usage- on demand- based model ensures that the Purchasing Entity is able to deal with seasonal and monthly peaks, only paying for that capacity when needed, without carrying the additional cost of an infrastructure that will meet peak capacity.

8.1.2.5 Measured Service

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

The Contact Solutions IVR product automatically controls and optimizes resource use by leveraging a metering capability. Information system resource usage can be monitored, controlled, and reported, providing transparency for both the provider and client of the utilized service.

8.1.3 Service model sub-categories offered

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

Contact Solutions intends to provide Software as a Service (SaaS) via private cloud with the following subcategories.

- Other – Interactive Voice Response

8.1.4 Willingness to comply with Attachments C&D requirements

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

Contact Solutions complies with the requirements of Attachments C and D.

8.1.5 Adherence to Scope of Services requirements

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

Contact Solutions' cloud-based SaaS IVR offering adheres to the services, definitions, and deployment models identified in the Scope of Services.

Contact Solutions manages the entire underlying cloud infrastructure, including network, servers, operating systems, storage, and individual IVR application capabilities. Our cloud infrastructure is provisioned for exclusive use by Contact Solutions, comprising of IVR applications for multiple clients. Our adherence to the five essential NIST characteristics is described above in Section 8.1.2.

The Contact Solutions production platform architecture is designed to ensure business continuity and system redundancy for all our customers' hosted applications, resulting in an actual availability greater than 99.9%. Contact Solutions employs a unique 3-way always-active architecture at the data center level. Three geographically dispersed, continuously linked, yet independently operable data centers automatically and dynamically balance call-handling load across all data centers.

Highlights of the architecture include:

- Call allocation across multiple, geographically diverse sites
- Call failover site-to-site
- Customer host transaction interfaces to and from all sites
- Independent application and database servers at each site
- Independent internet and private data network access from each site
- Multiple voice and data network providers at each site

Additional fault tolerance features are implemented within each data center, designed to eliminate single points of failure. Computers, servers and network equipment are deployed in an 'N+1' redundant configuration at each layer of the solution architecture.

8.2 Subcontractors

8.2.1 Whether to use 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.

Contact Solutions personnel perform all professional services associated with the delivery of client IVR solutions, including:

- Project management.
- Custom application, network and integration design.
- IVR development, system logic and host integration software development.
- Carrier network integration.
- Report development.
- Deployment to cloud platform.
- Platform operations, administration, management and provisioning.
- Continuous improvement monitoring and recommendations.
- Ongoing application and software changes.
- Contract management.

Contact Solutions relies upon subcontracted voice talent for voice recordings in English, Spanish, and other languages as specified by our clients.

8.2.2 Extent of use of subcontractors

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

Contact Solutions personnel perform all professional services associated with the delivery of client IVR solutions, with the exception of professional voice talent required to record IVR messages. Voice talent subcontractors produce voice files in standard formats that are then loaded onto the IVR platform by Contact Solutions personnel only.

Contact Solutions relies upon subcontracted voice talent for voice recordings in English, Spanish, and other languages as specified by our clients. Our project management personnel engage the appropriate voice recording company based on specific needs of the client and coordinate all aspects of the recording process in accordance with the client's requirements. Voice talent subcontractors produce voice files in standard formats that are loaded then onto the IVR platform by Contact Solutions personnel only.

8.2.3 Qualifications of subcontractors

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

Contact Solutions has worked with the following industry leading companies for years to deliver high quality voice recordings to meet our clients' needs.

- [redacted] was founded in 1985. Originally, the company developed radio commercials and professional phone voice recordings for business applications such as Voice Mail and Auto Attendant applications. Their staff provides Voice Project Management for a variety of applications, and includes Persona Design, Touch Tone and Speech Rec IVR support, Call Center recording support, web audio, audio for professional communications and eLearning.
- [redacted] has emerged as the global leader in professionally-recorded voice for automated voice technologies including IVR, auto attendant, call routing, even in-car GPS and telematics applications.
- [redacted] For more than 20 years, [redacted] has been dedicated to providing digitized custom voice files in a multitude of formats and in more than 35 languages.

We will ensure these subcontractors will meet SOW requirements by working closely with the Purchasing Entities to get their approval of both the scripts and the actual voice recordings before deploying them in the IVR.

8.3 Working with purchasing entities

8.3.1 Data breaches

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

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

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

In support of the NASPO contract, Contact Solutions shall operate a formal incident response capability consistent with all State and Federal law as applicable under this contract. Contact Solutions is prepared to handle any incident, and we place special emphasis on incidents that use common attack vectors. Staff training and organizational policies and procedures emphasize the importance of incident detection and analysis throughout the organization.

Contact Solutions reduces the frequency and potential severity of incidents by effectively securing networks, systems, and applications. We address potential risk proactively to protect the information system and client and citizen data. Guidelines for interactions with other organizations regarding incidents will be established and tailored to meet the specific requirements of NASPO and all Participating Entities. Contact Solutions has developed mature, tested logging standards and procedures

to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly.

Contact Solutions employs written guidelines for prioritizing incidents, which is a critical decision point in the incident response process. Effective information sharing can help an organization identify situations that are of greater severity and demand immediate attention. We use the lessons learned process to gain value from incidents; the information accumulated from lessons learned meetings is reviewed by management and to addresses systemic weaknesses or deficiencies in policies, procedures, and education.

Contact Solutions employs a Computer Security Incident Response Plan (CSIRP) to ensure timely and effective handling of all situations. The CSIRP is reviewed and updated on an annual basis to ensure it is current and accurate. Changes made to the plan are communicated to the incident response team along with proper training. The CSIRP is developed and consistent with *NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide* and industry best practices.

The CSIRP Team:

- Serves the Purchasing Entity and the entire Contact Solutions organization and its systems and applications.
- Is responsible for responding to all computer security incidents with the goal of minimizing the impact on customer and Contact Solutions' business operations, applications, systems and security.
- Notifies and aligns with customers' incident response requirements, including reporting, investigation or forensics, and root-cause analysis.
- Responds to all incidents affecting Contact Solutions' system components to resolve any incidents.
- Conducts an analysis of legal requirements for reporting compromises and responds accordingly.
- Conducts lessons learned sessions post-incident to improve internal processes, augment control implementation, and remediate deficiencies, for each contributing factor to the incident.
- Reviews policy developments and updates, if appropriate, to ensure against future incidents.
- Develops new or enhances existing security training materials for staff and end-user education, as appropriate.
- Provides timely staff training.

Organizational Structure / Roles and Responsibilities

- CSIRP Team Manager: Mike Rodway, Sr. Manager Engineering and Operations

  The CSIRP Team Manager (Manager) is responsible for overall response and recovery activities for all security incidents. The Manager determines along with the Assistant to the CSIRP Team Manager the severity of the incident and the action to be taken to facilitate recovery. The Manager determines which team members to call upon to assist in the recovery process. The Manager oversees all

decision-making authority to take necessary actions during and after an incident. The Manager reports to the Management Advisory Board. (See below.)

- Assistant to CSIRP Team Manager: Jeff Ormsbee, Principal Security Engineer

  The Assistant to the CSIRP Team Manager (Assistant) is responsible for working with the Manager to determine the actions necessary to facilitate data and systems recovery. If the Manager is not available, the Assistant assumes all Manager responsibilities. The Assistant follows up on any policy and procedure documentation and testing that must be created due to the incident and the recovery process. Communication regarding new policy/procedural changes takes place with the Team Manager.

- Management Advisory Board: led by Chris Sussman; Sr. Vice President of Operations

  The Management Advisory Board is responsible for providing decision-making resources that are required above what the CSIRP Team Manager is authorized to implement.

Permanent Team Members are responsible for assisting in the implementation of the recovery plan as directed by the CSIRP Team Manager and/or the Assistant CSIRP Team Manager. Team members test recovery plan annually or upon significant change, and document any new and/or changed policies and procedures due to the incident. Team members forward documentation to the Assistant Team Manager.

Temporary Team Members are responsible for participating in the incident response as requested by the Team Manager or the Assistant Team Manager. Team members assist the recovery process based on their areas of expertise and experience. Team members are involved in creating and/or updating business policy and procedures as requested by the Manager or the Assistant.

The Team Manager and Assistant Team Manager report all incidents and findings to the Management Advisory Board.

All Permanent Team Members, if called upon to assist in the incident, report to the Team Manager or if unavailable, the Assistant to the Team Manager.

Temporary Team Members, if called upon to assist in the incident, are notified by Team Manager and Assistant to Team Manager.

Designated personnel are available on a 24/7 basis to respond to risk alerts.

Incident Declaration/Information Flow

When an incident requiring CSIRP Team activation occurs, a formal incident is declared. The incident is brought to the immediate attention of the CSIRP Team Manager and the Assistant Team Manager. A decision is made regarding the severity level of the incident. The selection of team members is made to assist in resolving the incident. If appropriate, the information must be shared with any outside

vendors affected by the incident, security organizations as required (i.e. US-CERT), and subsequent resolution.

Breach Notification

Notification will be triggered upon "reasonable belief" that sensitive data has been acquired by an unauthorized person. Sensitive data includes, but is not limited to, Payment Card Industry (PCI) data, Health Insurance Portability and Accountability Act (HIPAA) data, Intellectual property data and Personally Identifiable Information (PII). Notification will be made by the Contract Manager without unreasonable delay following the discovery of a security breach.

Response Phases

Alert Phase

The Alert Phase is the process of learning about a security incident or the potential of a security incident and reporting it verbally to the CSIRP Team Manager or Assistant Team Manager. Alerts may be identified via firewalls, intrusion detection systems, intrusion prevention systems, file integrity monitoring systems, anti-virus software, threats via electronic mail, media reports etc.

Contact Solutions monitors critical security breach indicators, such as:

- Windows event logs
- File integrity monitor reports
- Firewall log reports

The Manager or Assistant opens the master bug via our Bugzilla tool to track the incident and all permanent team members are copied on the bug.

The 24/7 Engineer On Call Employee Directory is used to reach team members. The person identifying the security incident should contact the Team Manager or Assistant Team Manager directly via their office and/or mobile phone numbers.

Triage Phase

The Triage Phase is the process of evaluating the information available regarding the incident to determine if it is a true incident and if so, the severity level. Evaluation is conducted by the CSIRP Team Manager and the Assistant Team Manager. The decision must be made whether the incident requires a resolution only, or if the incident must be reported to local authorities for a criminal investigation. Financial and personnel resources are identified. If the level of the incident warrants, the Management Advisory Board is notified along with any Permanent Team Members and Temporary Team Members.

Response Phase

CSIRP Team gathers all evidence to include, but not limited to an audit trail, log files, contents of files etc. Once evidence has been gathered, analysis is performed to determine the cause of the incident and the vulnerability to Contact Solutions' operations, systems and applications. An assessment is made to determine how far

the vulnerability has spread. A resolution is determined to secure all operations, systems and applications.

If a criminal investigation is required, the appropriate authorities are contacted immediately to ensure that the evidence is maintained in a manner that will allow it to be admissible in a court of law.

Recovery Phase

The Recovery Phase begins immediately upon completion of the Response Phase. The CSIRP Team begins restoring the systems and applications affected by the incident. The recovery may include, but is not limited to reloading data or reinstalling systems. Testing must be completed during the recovery process to ensure that all systems and applications are running at their original capacity.

The outcome of the Recovery Phase will be a series of change requests logged in Bugzilla at the appropriate incident severity level. These change requests are then planned, executed and tested as per Contact Solutions' standard engineering processes. The 'depends on' and the 'blocks' features will be used as appropriate.

The Recovery Phase encompasses the resolution and conclusion of the master bug and all associated incident bugs.

Maintenance Phase

The Maintenance Phase requires the CSIRP Team to evaluate the response, recovery, team involvement, policies and procedures. The areas that require improvement are addressed with appropriate team members, new process documentation is created and implemented, and the CSIRP is updated according to lessons learned. Additionally the CSIRP must be updated to incorporate industry developments.

Incident Documentation

Contact Solutions' Team Manager or Assistant Team Manager must document each incident that occurs regardless of severity level. The Manager or Assistant are required to communicate the incident to the Management Advisory Board along with all specifics regarding the incident, level of damage, required team involvement and incident resolution. The Manager or Assistant is also responsible for contacting any vendors, contractors or other authorities if deemed appropriate by the Management Advisory Board. The Manager or Assistant must complete an Incident Report Form and forward to the Vice President/Chief Operations Officer. An electronic copy of the Incident Report Form must then be attached to the master bug and a hard copy filed in the Management Advisory Board's office at the conclusion of the Recovery Phase.

8.3.2 Prohibit adware, software, marketing

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.

Contact Solutions complies with this requirement. We will not engage in nor permit our agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Contact Solutions performs many government contracts with the same or similar kinds of prohibitions on adware, software, and marketing and we understand the importance of fully abiding by strict public-service contract requirements.

8.3.3 User test/staging environment identical to production

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

Contact Solutions complies with this requirement. Our standard practice for delivering a solution includes a User Acceptance Period that meets the Purchasing Entity's specific requirements. We provide the Purchasing Entity with a test environment that replicates the production environment including access to a test host environment so complete end-to-end testing can be performed.

All system modifications go through a comprehensive testing and acceptance protocol. The testing cycle includes several stages. During all testing activities Contact Solutions prohibits the use of live production data for testing and development.

Once the test plan is created and the solution is ready for test, the following test cycles are applied:

- Test Prep: The overall test plan and individual test cases are created; test and UAT environments are setup and configured.
- Unit Testing: The development team tests the application, creates bugs that represent typical issues, and then retests until all issues are resolved.
- Development Integration Testing: The Integration Test team performs integration testing to ensure all data connectivity and host integrations are working properly.
- System Testing: The System Testing cycle, coordinated by the project manager, includes full application and integration testing, testing of failure conditions, testing of secure communications, validation of input and output, and encryption and data masking when appropriate.

We use the [redacted] Web Vulnerability Scanner for all new and modified web application code to ensure Open Web Application Security Project (OWASP) compliance. These scans check for cross-site scripting, SQL injection, malicious file

execution, information leakage and error handling, and authentication and session management. No code will be released to production until it is deemed PCI compliant.

[redacted] is used to test performance on both static and dynamic application resources. The tool simulates a heavy load on application components to test its strength and to analyze overall performance under load.

- User Acceptance Testing: Once the internal QA process is complete, the application is deployed to the User Acceptance Testing environment. During this phase, the Purchasing Entity vigorously tests the application and reports any issues.
- Regression Testing: Upon the resolution of any issues found during testing, the application is then regression tested with the new fixes to ensure the strength of the overall system. Once the application is tested by the Purchasing Entity, a formal sign off is completed.
- Production Integration Testing: The project team works with the Purchasing Entity to ensure that all production data connectivity and host integrations will work in the production environment.

8.3.4 Accessibility to users with disabilities

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

Contact Solutions will work closely with Participating Entities to ensure that our IVR solutions function as a fully integrated part of their ADA-compliant communications programs.

It is technically possible for the IVR platform to respond to TDD/TTY devices but it is not recommended. Providing user responses in TDD/TTY format is similar to duplicating the IVR call flow in an additional language; adding significant effort and associated cost to the initial application development effort as well as ongoing application improvements.

Our experience deploying hundreds of applications for state government programs indicates that the use of TDD/TTY devices is extremely low with the advent of text messaging, chat and web-based customer support. We recommend publication of a separate phone number for hearing or vision impaired citizens, which is directed to a number or group of numbers that are answered by agents with TDD/TTY devices or software.

8.3.5 Browser accessibility

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

Contact Solutions complies with this requirement. Our applications and content delivered through web browsers are accessible via current released versions of Internet Explorer, Firefox, Chrome, and Safari. Each software release is tested on each browser operating system prior to release into the production environment. During the Requirements phase, the (product/development) manager will verify the approved standard browser and versions with the Purchasing Entity to ensure compatibility.

8.3.6 Storage of sensitive information

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.

Contact Solutions complies with this requirement. Prior to the execution of a Service Level Agreement, we will meet with the Purchasing Entity to determine whether any sensitive or personal information will be stored or used by Contact Solutions that is subject to any law, rule, or regulation providing for specific compliance obligations. Data sensitivity and protection requirements are then translated into system and integration requirements for the solution design. This steps allows our information architects and system engineers to build the data confidentiality and privacy into the initial design.

Based on the importance of data protection and privacy for today's information systems, our solution designs are flexible in able to respond to changes in legislation and requirements as needed.

8.3.7 Project schedule plans

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.

We assign a dedicated Project Manager to manage delivery of every solution from inception to production rollout and post-production support, which includes discovery, documenting, development, testing and implementation. We also require that we receive written acceptance by authorized Purchasing Entity staff for each stage of the project before we consider it complete.

The business objectives, requirements and ultimate delivery of each application go through a rigorous delivery lifecycle, which includes:

- Planning and Administration – assignment of management and coordinating of all facets of the delivery process.
- Discovery - during this phase, the team meets to understand the existing contact center solution, and if it exists, the existing solution to support a detailed requirements gathering phase later in the delivery cycle including performance baseline and security review.
- Requirements - detailed requirements are defined by the Purchasing Entity and our project team for final review and signoff and include:
    - Performance baseline
    - Business requirements & analysis
    - Reporting requirements
    - CTI requirements
    - Data access requirements
    - Host integration points
    - Telecom requirements
    - Solution monitoring
- Design - design is an essential phase prior to the start of Development and Implementation. During this phase, the requirements are translated into a design that will support the solution.
- Development and Implementation - the Development and Implementation phase encompasses development of databases, the custom application, reports, the client host data access and telecom.
- Testing - the testing cycle includes several stages. During all testing activities Contact Solutions prohibits the use of live production data for testing and development. Once the test plan is created, the solution is ready for testing. Please refer to 8.3.3 for a detailed description of our test environment.
- Deployment - in the Deployment Phase, we deploy the IVR application to the production ports and resources and move the volume to the application.
- Post Production Support - consists of monitoring the application and includes evolutionary changes to the application as requirements grow and business purposes change.
- Continuous Improvement – through further customization we focus on improving customer satisfaction and automation.

Because of the nature of the technology, deliverables for each solution will be provided to the Purchasing Entity in preliminary form in multiple formats for review and written approval prior to beginning work on actual deliverables. Each delivery goes through a formal process to enable the Purchasing Entity appropriate review and comment. Examples include:

- Script and call flow and/or web flow requirements are provided by the Purchasing Entity. Contact Solutions will deliver draft diagrams using Microsoft Visio software for review. Comments are reviewed and a final script and call flow and/or web flow are documented for acceptance by the Purchasing Entity before our staff begins development of the application.
- Call recordings are submitted to the Purchasing Entity for review and approval before they are converted and deployed to the platform.
- All available standard reports are provided to the Purchasing Entity for discussion and review, and standard reports are finalized in discussion with the Purchasing Entity.
- Custom reports are based upon requirements analysis, and proposed reports are submitted to the Purchasing Entity for review and approval prior to development.
- All change requests involving deliverables go through analysis, and proposed deliverables are submitted for review and approval by the Purchasing Entity.

We will provide the Purchasing Entity with copies of new deliverables for review and approval, including call flows, reports, screens, and other deliverables, and revised materials, as they are updated. Any deliverables for which the Purchasing Entity desires a walkthrough for clarification and/or to address any deliverable issues prior to submission for final approval will be provided upon request.

Contact Solutions' standard practice for delivering a solution includes a User Acceptance Period. The Purchasing Entity is provided with a test environment that replicates the production environment including access to a test host environment so complete end-to-end testing can be performed.

Contact Solutions will develop an interface to the host database. We assume that the Purchasing Entity's personnel or their designees provide all necessary specifications, test environments, test data and access to expertise necessary to develop and test the interface.

We have included a sample project plan as a separate file entitled Contact Solutions Sample Project Plan.

8.4 Customer Service

8.4.1 How to ensure excellence

8.4.1 Offeror must describe how it ensure excellent customer service is provided to Purchasing Entities. Include: • Quality assurance measures; • Escalation plan for addressing problems and/or complaints; and • Service Level Agreement (SLA).

We assign a dedicated Project Manager to manage delivery of every solution from inception to production rollout and post-production support, which includes discovery, documenting, development, testing and implementation. We also require that we receive written acceptance by authorized Purchasing Entity staff for each stage of the project before we consider it complete.

The business objectives, requirements and ultimate delivery of each application go through a rigorous delivery lifecycle as described in 8.3.7.

End-to-end application performance is as critical as platform reliability. Our engineering team monitors and pro-actively manages our end-to-end self-service solutions including telecom, host systems and cloud platform. To date, we have always met our SLA commitments – every time. Contact Solutions will work with individual Purchasing Entities to define agreed upon SLAs. In general, Contact Solutions adheres to a 99.999% service level.

Contact Solutions provides a complete monitored solution for customers using our own internal Network Operations Center (NOC). The NOC monitors the cloud components and services on a 24x7x365 basis and provides custom-tailored alerts to issues or service degradation directly to the customer, allowing for personalized notification and escalation.

In order to ensure support for unexpected spikes in call volume, Contact Solutions maintains 100% reserve capacity in its active IVR footprint. Our Operations team monitors network utilization and plans system capacity and port availability well in advance of expected volume increases. If utilization begins to exceed 50% of system capacity on a typical day, expansion plans are executed. Forecasting reports linked to our platform automatically notify our purchasing team when it is time to add additional platform capacity. Because we are deployed in [redacted] data facilities and are never constrained by the size of company-owned data centers, there is virtually no limit to our ability to add capacity as required.

Purchasing Entities will have a single point of contact for all questions and issues that may arise during implementation. That point of contact will be the project manager, who will manage development and implementation of the IVR solution, ensuring a full, end-to-end understanding of the intricacies of the Purchasing Entity and the application. The project manager will engage other Contact Solutions resources as necessary.

Post-implementation, Purchasing Entities will have access to our Client Help Desk which provides a dedicated team to respond to requests for application support. This team will be responsible for documenting, escalating (as required), resolving, confirming a satisfactory resolution, and closing all support requests.

Our Engineer on Call (EOC) provides 24 x 7 x 365 support via a centralized pager number. The EOC is available to Purchasing Entities for service-impacting issues outside of normal business hours. Both the Client Help Desk and the EOC have access to all Contact Solutions resources, including the project manager, and will escalate as necessary to resolve the issue.

8.4.2 Compliance with customer service requirements

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:	
RFP requirement	**Contact Solutions compliance**
a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.	Contact Solutions complies with this requirement. We will provide a Project Manager as the single point of contact for each Participating Entity.
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.	Contact Solutions complies with this requirement. In addition to the Client Help Desk, which is available during normal business hours, our Engineer on Call (EOC) provides 24 x 7 x 365 support via a centralized pager number. The EOC has access to all Contact Solutions resources.
c. Customer Service Representative will respond to inquiries within one business day.	Contact Solutions complies with this requirement. We will respond to all inquiries from a Participating Entity within one business day.
d. You must provide design services for the applicable categories.	Contact Solutions complies with this requirement. We will provide design services for our SaaS IVR solution.
e. You must provide Installation Services for the applicable categories.	Contact Solutions complies with this requirement. We will provide installation services for our SaaS IVR solution as applicable.

8.5 Security of Information

8.5.1 Data protection

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.

Data Security

Contact Solutions builds and manages IVR solutions for its clients that frequently read or write data elements. Occasionally, data that is being processed may be considered sensitive or secure. Contact Solutions utilizes various methods to ensure secure data transmission and storage.

Payment Card Holder Data Management

For some government programs, Contact Solutions collects and processes card holder information and other sensitive client data.

Card holder data shall only be collected and processed inside the designated PCI secure network segment.

Our solutions and their related host integration, CTI and associated software components are designed, developed, reviewed and tested to ensure no card holder or other sensitive data is stored by the IVR in log files or database tables.

The use of cookies for web session management is prohibited within applications collecting sensitive information.

Card Holder Data Access

Access to any card holder data is on a need-to-know basis only. Approval for access must be requested in writing from the Contact Solutions Chief Security Officer.

Data Transmission and Encryption

Contact Solutions has multiple methods to transport data securely:

- Encrypted VPN tunnels
- Private Data Circuit
- Secure HTTP transmission using certificates
    - Latest SSL encryption required for transmission
    - HTTPS is required in the URL
- Secure FTP

Data Storage

Contact Solutions stores non-sensitive client related data locally within the platform database infrastructure. Our platform architecture allows sensitive data to be segmented on physically separate database servers if required.

Additionally, Contact Solutions mandates data masking techniques to ensure that data (i.e. account numbers, SSN, etc.) is stored securely and without manual inspection. Contact Solutions allows for the storage of the first 6 digits or the last 4 digits of sensitive card data, but not full Personal Account Number (PAN) or credit card number. Storage of both within the same application is prohibited.

Contact Solutions prohibits the storage of credit/debit card track data, CVV2 and PIN codes.

Data Encryption Key Management Policy

Contact Solutions implements encryption of customer sensitive information by using a two-tiered encryption architecture. Sensitive information is encrypted using a symmetric AES_256 encryption key and stored in a separate database.

The AES_256 encryption key is further encrypted using a certificate generated with the database master encryption key (key-encrypting key). Full password to the AES_256 encryption key is not known by any one individual and is stored on the database server in an unreadable format. All backup encryption keys are centrally stored on a secure management server.

Data Disposal

Contact Solutions utilizes [redacted] Secure Media Destruction Service for disc and tape destruction. Benefits of the service include:

- Secure transportation of sensitive information
- Trained and rigorously screened personnel
- Accountability with a documented chain-of-custody
- An environmentally friendly waste-to-energy incineration process that also ensures complete media destruction

8.5.2 Compliance with applicable laws

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

Contact Solutions complies with this requirement. We intend to comply with all applicable laws related to data privacy and security.

The Contact Solutions security team subscribes to alerts from Multi-State Information Sharing and Analysis Center (MS-ISAC), National Conference of State Legislatures (NCSL), United States Computer Emergency Readiness Team (US-CERT), Center for Internet Security (CIS), Federal Risk and Authorization Management Program (FedRAMP), Cloud Security Alliance (CSA), Defense Information Systems Agency (DISA), NIST Computer Security Resource Center, and the SANS Institute to remain current on changes in legislation, threats, advisories, security trends, and information necessary to protect the information system. The U.S. Department of Homeland Security has designated the MS-ISAC as its key cyber security resource for State, Local, Tribal and Territorial governments. The NCSL provides resources that help to monitor changes in regulatory requirements by state.

8.5.3 Purchasing Entity's user accounts or data

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.

Contact Solutions complies with this requirement. We 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.

8.6 Privacy and Security

8.6.1 Compliance with NIST SP 800-145

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.

Contact Solutions' Interactive Voice Response (IVR) product offers a Software as a Service (SaaS) solution via private cloud, which is fully compliant with NIST Special Publication 800-145, The NIST Definition of Cloud Computing.

The IVR capability provided to the client uses Contact Solutions' applications that run on a cloud infrastructure. The client does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage. Individual application capabilities, limited to user-specific application configuration settings, are accessible from various client devices through a web browser. The IVR SaaS can be interfaced to connect directly to the clients' information systems to drive response, collect data, or support other client requirements.

The IVR product is deployed as a private cloud. The cloud infrastructure is provisioned for exclusive use of each client. It is managed and operated by Contact Solutions, and it exists off premise in three certified data centers, geographically disbursed in the continental United States.

The IVR solution has broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., telephones, mobile phones, voice over IP, tablets, laptops, and workstations). Contact Solutions' computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

The IVR capabilities can be elastically provisioned and released, automatically, to scale rapidly outward and inward commensurate with demand. The Contact Solutions IVR product automatically controls and optimizes resource use by leveraging a metering capability. Information system resource usage can be monitored, controlled, and reported, providing transparency for both the provider and client of the utilized service.

8.6.2 Security certifications

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.

Contact Solutions employs rigorous, documented, implemented, and monitored security standards, which have been and continue to be reviewed as part of a Level 2 SSAE-16 audit and PCI compliance review. We are SSAE-16 certified and PCI and HIPAA compliant.

Contact Solutions constructs all policies and procedures leveraging FISMA, NIST SP 800-53, NIST SP 800-37, and other relevant NIST guidance. Contact Solutions is currently evaluating submission of a FedRAMP package, which also certifies FISMA and NIST SP 800-53 compliance.

8.6.3 Security practices

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.

Contact Solutions' executive management fosters and continuously drives a security culture. The security management approach consists of nurturing a security-conscious organizational culture, developing tangible procedures to support security, and managing assets that comprise the information system. A proactive and results-oriented security culture is one of the single most critical core competencies within an organization.

Contact Solutions emphasizes security within all functional areas of product delivery to our clients. Our staff builds information assurance best practices into each phase of the System Development Life Cycle (SDLC).

Contact Solutions' people, policies, and processes deliver effective information system security as a result of a workplace environment and organizational structure where management understands and fully supports security efforts, and users are encouraged to exercise open communication and due diligence.

Levels of Security Control

Contact Solutions manages access to the IVR platforms using a combination of industry standard firewall technology, key fob RSA security tokens, VPNs and account name/password user login management.

Penetration Testing and Vulnerability Scanning

Contact Solutions conducts external penetration testing annually or after any significant change to the externally accessible environment. Penetration testing must be performed by qualified individuals and requires network and application layer testing. We retest as necessary until passing results are obtained.

Contact Solutions conducts external vulnerability scanning quarterly or after any significant change to the externally accessible environment. External vulnerability scans must be performed by an authorized scan vendor (ASV). We rescan as required until passing results are obtained.

Contact Solutions requires internal vulnerability scanning occur quarterly, or after any significant change to the environment, and throughout the development process. In addition, vulnerability scans are performed on all card data environment (CDE) systems. Remediation occurs immediately after testing is completed. Failing systems are rescanned until a passing report is produced.

Operations staff performs quarterly scans and open troubleshooting tickets for any findings. Troubleshooting tickets are assigned to the engineering staff for remediation and testing.

Intrusion Detection System (IDS)

Contact Solutions has implemented a network intrusion detection system that reads all inbound and outbound data packets to detect suspicious activity. The IDS is a dedicated Cisco/Sourcefire appliance capable of performing packet logging and real-time traffic analysis.

Network Firewalls

Contact Solutions will use stateful packet inspection firewalls in a redundant state to control access to CS networks. We place firewalls at all border entry points to our networks, all DMZ segments and all entries to secure environments. Contact Solutions requires the use of Network Address Translation (NAT) to mask all private IP addresses prior to leaving a Contact Solutions network. Any disclosure of private Contact Solutions IP addresses and routing, to external parties must be authorized by Engineering and Operations managers. All configuration changes must follow our standard change control process for network firewall devices.

VPN Platform Access

A firewall limits traffic to the Contact Solutions servers via VPN connections. The VPN client software program is installed and enabled on the user's computer; firewall access requires a user ID and password. After VPN connection to a specific asset, unique username/password pairs are then required to gain access to the Contact Solutions platform environment.

Contact Solutions standard anti-virus software with up-to-date virus signatures, real-time scanning, active firewall and URL filtering is required for systems with access to the Contact Solutions secure environment.

Only Contact Solutions owned and issued equipment is allowed access to any secure environment.

Only employees listed on the Contact Solutions SharePoint portal within the Engineering and Operations group will be allowed access to the production secure environment.

Password Management and Control

Network device access is controlled by individual user accounts configured on each device. User passwords must adhere to the documented Contact Solutions Password Policy.

Critical servers, including the interface to the IVR applications and database servers, require additional login access controls that provide an incremental level of control. An administrator-level user ID and password is required to gain access.

Virus Detection and Protection

Symantec Anti-Virus protection and detection software is installed on Windows OS systems. The anti-virus software is configured to receive automatic virus definition updates. The real-time virus scan protection option is enabled.

Network Device Security Log Management

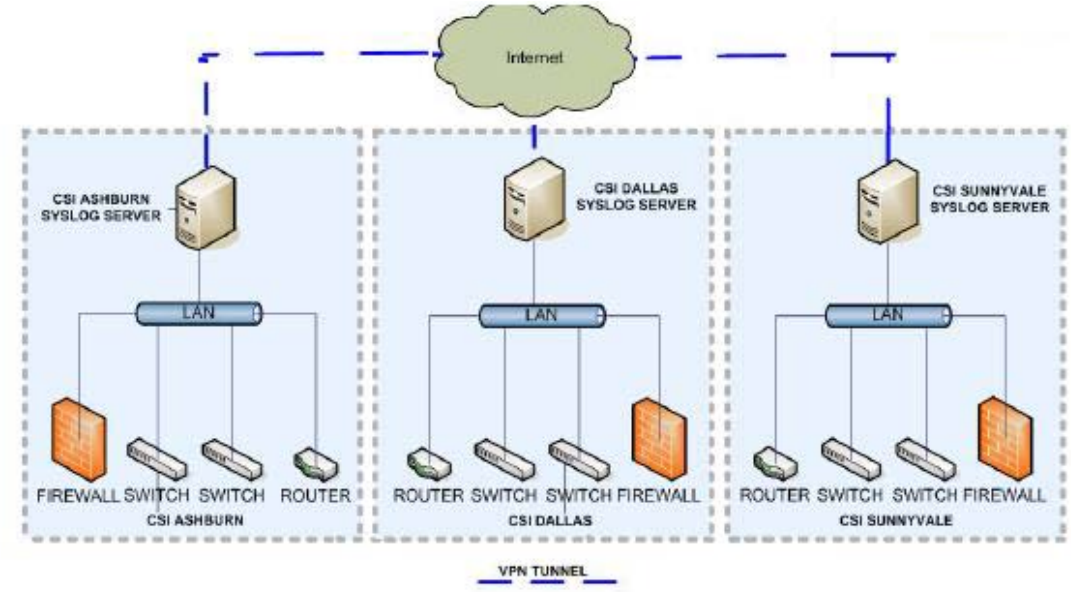
Contact Solutions enables within its IVR platform a centralized syslog storage and management system. Logs from network devices are sent to the syslog server on its local LAN segment.

The security logs are reviewed (either as a result of automated alerts or manual inspection) on a daily and weekly basis dependent on the log type. Logs are archived daily and weekly. Logs are kept for one week before being stored as historical files for one month. After one month, files are then archived to tape. Archived log files are purged after 12 months. Logs include the user name, IP address, and session time.

All logs generated by systems processing card data are kept for a full week before being stored as historical files for one month. After one month, files are archived to tape and stored for one year.

These centralized syslogs are inspected periodically in accordance with Contact Solutions' security policies.

Figure 2: IVR Platform Syslog Management System



Client Site-to-Site Network Integration

Client applications running on the Contact Solutions hosting platforms can integrate locally or remotely with client data. These integrations are accomplished via secure transmission over the public Internet or private data networks.

Data transmitted across a VPN are encrypted using standard IPSEC 3DES or AES-256 encryption. All private point-to-point frame and MPLS integrations come through a DMZ. Network segmentation by client within the Contact Solutions DMZ is accomplished using VLAN configuration.

Client connections via the public Internet are implemented across a VPN or use secure HTTP. In some instances, client data is transmitted and received in a batch configuration via secure FTP.

8.6.4 Confidentiality standards and practices

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).

Contact Solutions implements a number of industry standard encryption methods for transferring data including AES-256. We will meet any additional requirements from the Purchasing Entity. Please refer to 8.5.1 for details on data security.

Only Engineering and Operations staff are authorized to access production systems. We review access on an ongoing basis and update it whenever roles and responsibilities change among Contact Solutions personnel.

We monitor and log all production systems activity. We restrict access to the Purchasing Entity's sensitive data to approved users with a legitimate business purpose. We encrypt all sensitive data as an added layer of security. All users will be authenticated and logged, and we maintain logs for at least 6 months.

We require all our employees to read and sign the Contact Solutions Security Operations and Procedures document, which includes an Acceptable Use Policy. Employees must sign-off on this policy on an annual basis. Upon termination of employment, change in role or responsibility, or any other factor that would alter the need for access to sensitive information, Contact Solutions immediately removes that person's access to sensitive data.

We conduct background checks on all Contact Solutions employees, including those with access to sensitive data. Additional measures for employees with access to sensitive data are:

- Added training on incident response
- Required 2-factor authentication
- Real-time alerting for logon/logoff events

8.6.5 Third-party security credentials

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

Contact Solutions utilizes our existing certifications to satisfy customer requirements. We employ rigorous, documented, implemented, and monitored security standards, which have been and continue to be reviewed as part of a Level 2 SSAE-16 audit and PCI compliance review. We are SSAE-16 certified and PCI and HIPAA compliant.

We will work with Purchasing Entities to determine if additional attestations are required.

8.6.6 Logging process

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

Contact Solutions enables, within its IVR platform, a centralized syslog storage and management system. Logs from network devices are sent to the syslog server on its local LAN segment.

The security logs are reviewed (either as a result of automated alerts or manual inspection) on a daily and weekly basis dependent on the log type. Logs are archived daily and weekly. Logs are kept for a full week before being stored as historical files for one month. After one month, files are then archived to tape. Archived log files are purged after 12 months. Logs include the user name, IP address, and session time.

All logs generated by systems processing card data are kept for a full week before being stored as historical files for one month. After one month, files are archived to tape and stored for one year.

These centralized syslogs are inspected periodically in accordance with Contact Solutions' security policies.

In addition to performing the necessary annual external audits for Payment Card Industry and SSAE-16 compliance, Contact Solutions will strategically implement additional logging and auditing controls as part of our continuous monitoring and process improvements to enhance our security posture and maintain security certifications.

8.6.7 Restricting visibility of data

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

Contact Solutions complies with this requirement. The information system architecture is protected by multiple firewalls to protect the confidentiality, availability, and integrity of the data, including the protection and isolation of sensitive data. All firewall changes require change management approval and follow the guidelines established by the *Contact Solutions Delivery Life Cycle, R. 3.1, January 8, 2016*.

In addition, every Contact Solutions IVR is built such that it can be securely administered through a web portal management tool. The Contact Solutions Optimization Portal employs role-based controls so viewing and changing system behavior can be restricted to specific logins and passwords. We will work with individual Purchasing Entities to define level of access for specific users or groups as required.

8.6.8 Incident notification process

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.

Contact Solutions employs a Computer Security Incident Response Plan (CSIRP) to ensure timely and effective handling of all situations. The U.S. Department of Homeland Security has designated the MS-ISAC as its key cyber security resource for State, Local, Tribal and Territorial governments. The NCSL provides resources that help to monitor changes in regulatory requirements by state. Contact Solutions will ensure that individual Purchasing Entity requirements for incident notification are consistent with applicable laws and data categorization.

Please see Section 8.3.1 for details on the CSIRP team and the notification process.

Incident Severity Levels

- Minor (1) - Small numbers of system probes or scans detected on internal systems, isolated instances of known computer viruses easily handled by anti-virus software.
- Normal (2) - Small numbers of system probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable.
- Major (3) - Significant numbers of system probes or scans detected or detection of one or more rogue wireless devices; penetration or denial of service attacks attempted with no impact on operations; widespread instances of known computer viruses easily handled by anti-virus software; isolated instances of a new computer virus not handled by anti-virus software.
- Critical (4) - Penetration or denial-of-service attacks attempted with limited impact on operations; widespread instances of a new computer virus not

handled by anti-virus software, some risk of negative financial or public relations impact.

- Blocker (5) - Successful penetration or denial of service attacks detected with significant impact on operations; significant risk of negative financial or public relations impact.

Incident Severity Required Response

Minor (1)

- Notify the CSIRP Team Manager and Assistant Team Manager in order to set the CSIRP in motion.
- Contain the damage. Disconnect affected systems from the network.
- Create and/or update applicable bugs and copy designated resources.
- Assign CSIRP Team Members to assist in response.
- Determine the severity and the exact nature of the incident and what systems and applications have been compromised.
- Rebuild / reload affected systems.
- Determine and install preventative measures on affected and all application systems.

Normal (2)

- Notify the CSIRP Team Manager and Assistant Team Manager in order to set the CSIRP in motion.
- Contain the damage. Disconnect affected systems from the network.
- Create and/or update applicable bugs and copy designated resources.
- Assign CSIRP Team Members to assist in response.
- Determine the severity and the exact nature of the incident and what systems and applications have been compromised.
- Rebuild affected systems or patch systems appropriately to correct suspected vulnerability.
- Determine and install preventative measures on affected and all application systems.

Major (3)

- Notify the CSIRP Team Manager and Assistant Team Manager in order to set the CSIRP in motion.
- Contain the damage. Disconnect affected systems from the network; in the case of wireless devices, after disconnecting remove them from the premises.
- Create and/or update applicable bugs and copy designated resources.

- Assign CSIRP Team Members to assist in response.
- Determine the severity and the exact nature of the incident and what systems and applications have been compromised.
- Replace systems with backup systems if applicable.
- Rebuild / reload operating system.
- In the case of wireless devices, after the device has been disconnected and removed from the premises, investigate the origin and owner of the wireless device and ban the device from the premises permanently.
- Determine and install preventative measures:
    - Install appropriate software to prevent future problems on affected and all systems.
    - Patch systems appropriately to correct suspected vulnerability.
    - Update anti-virus software in order to handle new computer viruses.
    - Determine the type of Denial of Service attacks and take appropriate measures:
        - Disable any services not needed.
        - Apply any patches available.

<u>Critical (4)</u>

- Notify the CSIRP Team Manager and Assistant Team Manager in order to set the CSIRP in motion.
- Contain the damage. Disconnect affected systems from the network.
- Create and/or update applicable bugs and copy designated resources.
- Assign all CSIRP Permanent Team Members and if required, any Temporary Team Members to assist in response.
- Determine the severity and the exact nature of the incident and what systems and applications have been compromised.
- Replace systems with backup systems if applicable.
- Rebuild / reload operating system.
- Determine and install preventative measures:
    - Install appropriate software to prevent future problems on affected and all systems.
    - Patch systems appropriately to correct suspected vulnerability.
    - Update anti-virus software in order to handle new computer viruses.
    - Determine the type of Denial of Service attacks and take appropriate measures:

- Disable any services not needed.
- Apply any patches available.

Blocker (5)

- Notify the CSIRP Team Manager and Assistant Team Manager in order to set the CSIRP in motion.
- Contain the damage. Disconnect affected systems from the network.
- Create and/or update applicable bugs and copy designated resources.
- Assign all CSIRP Permanent Team Members and if required, any Temporary Team Members to assist in response.
- Determine the severity and the exact nature of the incident and what systems and applications have been compromised.
- Replace systems with backup systems if applicable.
- Rebuild / reload operating system.
- Determine and install preventative measures:
    - Install appropriate software to prevent future problems on affected and all systems.
    - Patch systems appropriately to correct suspected vulnerability.
    - Update anti-virus software in order to handle new computer viruses.
    - Determine the type of Denial of Service attacks and take appropriate measures:
        - Disable any services not needed.
        - Apply any patches available.

Incident Documentation

Contact Solutions' Team Manager or Assistant Team Manager must document each incident that occurs regardless of severity level. The Manager or Assistant are required to communicate the incident to the Management Advisory Board along with all specifics regarding the incident, level of damage, required team involvement and incident resolution. The Manager or Assistant are also be responsible for contacting any vendors, contractors or other authorities if deemed appropriate by the Management Advisory Board. The Manager or Assistant must complete an Incident Report Form and forward to the Vice President/Chief Operations Officer. An electronic copy of the Incident Report Form must then be attached to the master bug and a hard copy filed in the Management Advisory Board's office at the conclusion of the Recovery Phase.

8.6.9 Security controls to isolate hosted servers

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.

Contact Solutions uses stateful packet inspection firewalls, in a redundant state, to control access to cloud networks. Firewalls are placed at all border entry points to Contact Solutions networks, all DMZ segments and all entries to secure environments, creating physical and virtual Zones of Control Architectures (ZOCA) to isolate servers. Contact Solutions requires the use of Network Address Translation (NAT) to mask all private IP addresses prior to leaving a Contact Solutions network.

Contact Solutions' data center hosting services are provided by [redacted], Inc. Contact Solutions utilizes [redacted]'s services for physically hosting and securing its IVR platform hardware and software. [redacted] is the largest global network-neutral data center company in the world, with facilities in 11 major cities across the United States.

Hosted Site Security

[redacted] provides several levels of security as outlined below:

- Visitors entering the [redacted] hosting facility must make an appointment via an authorized CS representative 24 hours in advance of their visit.
- The Contact Solutions representative schedules an appointment via the [redacted] Internet portal or by calling the customer service help desk.
- Fourteen Contact Solutions employees are authorized to access the facility.
- Twelve of these employees are designated administrators.
- Only administrators have the ability to open appointment tickets, authorize equipment to be brought on-site, order cross-connects, etc., within the facility.
- No external technologies may be connected to or used within the PCI network segment. This includes email, flash drives, external hard drives and all similar technologies.
- Use of external storage devices used outside the PCI network segment, such as flash drives and external hard drives, must be scanned for viruses prior to use.
- External storage devices used outside the PCI network segment must be used solely for business purposes and cannot contain personal data.

Contact Solutions designated management staff maintain the list of employees authorized to enter the facility.

While in the facility, visitors must be accompanied by the Contact Solutions representative who made the appointment. Both the representative and the visitor are required to show picture ID and sign a logbook upon entering the facility. Contact Solutions representatives and visitors are issued [redacted] visitor badges by

the [redacted] security staff. These badges must be worn and shown at all times. Visitors shall not travel around the hosting facility unaccompanied. The sign-in and badge distribution functions are handled by [redacted] security guards. Badges must be returned to the [redacted] security guards upon the conclusion of the visit as per [redacted] policy.

Physical access to the facilities and the corresponding equipment cages containing the servers is controlled by a series of biometric hand scanners. The biometric hand scanners also require entry of a five-digit PIN. There are a total of five hand scanners between the front door of the hosting facility and the Contact Solutions equipment cages. The second of the five hand scanners can only be operated by the security guards and requires access via a mantrap prior to entering the main room.

The Contact Solutions equipment cages or equipment racks are also locked individually. The rack keys are in the possession of the Contact Solutions System Administrators. Only Contact Solutions employees who have been previously authorized for hand scan access are authorized to operate the hand scanners. Employees are allowed three attempts to authenticate to the hand scanner before the system locks them out and [redacted] security must reset their PIN. Audit trails of the hand scanners are maintained by [redacted] for a six-month period and can be reviewed on request from the authorized Contact Solutions representative.

Color, high resolution digital video surveillance cameras are in place (approximately 900) throughout the facilities, and video tapes are stored on-site. The Contact Solutions equipment cages have two security cameras – one monitoring each side of the rack.

8.6.10 Security Technical Reference Architectures

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)

Contact Solutions IVR SaaS aligns its security technical reference architecture to *NIST SP 800-53 (Rev. 4): Security and Privacy Controls for Federal Information Systems and Organizations security control families* as recommended in *NIST SP 500-293 Vol. 2 (Draft): US Government Cloud Computing Technology Roadmap Volume II: Useful Information for Cloud Adopters*. In a SaaS cloud Ecosystem, the cloud client (consumer) has only limited administrative control of the applications use and minimal control of the cloud and its Security Components. Contact Solutions is responsible to manage and secure all aspects of the solution and its implementation within the information system boundary.

Contact Solutions builds the following critical areas into its security model:

- Secure Cloud Ecosystem Orchestration
    - Deployment & Service Layers
    - Resource Abstraction and Control Layer (Hardware & Facility)

  - Physical Resource Layer (Hardware & Facility)
- Secure Cloud Service Management
  - Provisioning and Configuration
  - Portability/Interoperability
  - Business Support
- Secure Organizational Support
  - Organization processes, policies and procedures

Contact Solutions addresses each of the above critical areas in developing its security approach to protect the confidentiality, integrity, and availability of the client data and the SaaS information system.

8.6.11 Security procedures

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.

Contact Solutions implements a number of industry standard encryption methods for transferring data including AES-256. Any additional requirements from the Purchasing Entity will be met by Contact Solutions.

Only Engineering and Operations staff are authorized to access production systems. Access is reviewed on a continuous basis with access updated as roles and responsibilities change amongst Contact Solutions personnel.

All production systems activity is monitored and logged. Access to Purchasing Entity sensitive data is restricted to users with a legitimate business purpose, and all sensitive data is encrypted as an added layer of security. Additionally, all users will be authenticated and logged. Logs are maintained for at least 6 months.

All employees are required to read and sign the Contact Solutions Security Operations and Procedures document, which includes an Acceptable Use Policy. Employees are required to sign-off on this policy on an annual basis. Upon termination of employment, change in role or responsibility, or any other factor that would alter the need for access to sensitive information, Contact Solutions immediately removes access to sensitive data.

Background checks are conducted on all Contact Solutions employees, including those with access to sensitive data. Additional measures for employees with access to sensitive data are:

- Added training on incident response
- Required 2-factor authentication
- Real-time alerting for logon/logoff events

8.6.12 Security measures and standards

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.

Contact Solutions procures encryption technology that is tested against requirements found in *FIPS PUB 140-2, Security Requirements for Cryptographic Modules*.

Contact Solutions manages encryption capabilities and key management through Microsoft SQL Server, which maintains a combination of public, private, and symmetric keys to protect sensitive data, which uses an AES 256 algorithm. This is an extensible solution, which allows infrastructure components need to communicate with each other via public networks over VPN or private networks for additional security. Encryption is used for all data in motion to protect data and virtual machine images during transport across and between networks, hypervisor instances, and data centers.

8.6.13 Data breach policies and procedures

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.

Please refer to 8.3.1 for a detailed description of our policies and procedures regarding notification and mitigation of a data breach.

8.7 Migration and Redeployment Plan

8.7.1 End of life activities

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.

Prior to the end of the contract term, Contact Solutions will work with the Purchasing Entity to ensure safe deprovisioning of any active IVR solutions.

The following Contact Solutions personnel are responsible for deprovisioning activities.

- Client Services Project Manager: Responsible for managing the deprovisioning of an application through various bugs and requested resources to provide support of removing platform components.

- Software Development: Responsible for creating release notes, content or scripts to remove platform components as well as providing guidance for the Project Manager to identify the components to be removed.
- Engineering & Operations: Responsible for executing the action items provided by the Project Manager to remove application associated components and telecom from the production platform.

During deprovisioning, IVR applications continue to benefit from our 3-way active site architecture ensuring full redundancy and security throughout the completion of the process. Please refer to 8.5.1 and 8.12.1 for a detailed description of data security and of our redundant architecture.

8.7.2 Return of data

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.

Prior to deprovisioning of any active IVR solutions, the Contact Solutions Contract Manager will work with the Purchasing Entity to determine the data delivery method that best suits the Purchasing Entity's needs. Call detail record data is generally delivered via a secure server; however, Contact Solutions can provide data via alternate methods as required. Upon deprovisioning, data will be delivered via the agreed upon method.

8.8 Service or Data Recovery

8.8.1 Responding to adverse events

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

8.8.1.a extended downtime

a. Extended downtime.

Contact Solutions hosts our applications on a robust platform using common off-the-shelf hardware. The platform is housed in [redacted] hosting facilities located in Virginia, Texas, and California. This enables us to effectively operate at 100% uptime with multi-site disaster recovery capabilities. Each site is a 'hot' disaster recovery site, so there is no downtime in shifting traffic between sites as upgrades and maintenance are performed. We load balance all traffic across the three sites to provide 24 x 7 availability and maximum flexibility.

8.8.1.b Unrecoverable loss of data

b. Suffers an unrecoverable loss of data.

Contact Solutions backs up and stores its platform data, database data and source code. All Contact Solutions' source code is maintained in a source-safe management configuration system. Platform data and software source code backups are performed and retained according to the following schedule:

Frequency	Backup Type	Retention Period	Site Location
Nightly	Differential	1 week	On-site
Weekly	Full	4 weeks	On-site
Monthly	Full	12 months	Off-site

In addition, exact binary images of TRMs that run the applications are created periodically. These images are stored on DVD media and can be used to replicate or reproduce a specific system as the platform grows and in the event of a single system failure.

8.8.1.c System failure

c. Offeror experiences a system failure.

The Contact Solutions production platform architecture is designed to ensure business continuity and system redundancy for all our customers' hosted applications. Contact Solutions employs unique 3-way always-active architecture at the data center level. Three geographically dispersed, continuously linked, yet independently operable data centers automatically and dynamically balance call-handling load across all data centers.

Highlights of the architecture include:

- Call allocation across multiple, geographically diverse sites
- Call failover site-to-site
- Customer host transaction interfaces to and from all sites
- Independent application and database servers at each site
- Independent internet and private data network access from each site
- Multiple voice and data network providers at each site

Additional fault tolerance features are implemented within each data center, designed to eliminate single points of failure. Computers, servers and network equipment are deployed in an 'N+1' redundant configuration at each layer of the solution architecture.

8.8.1.d Recover, restore data in 4 hours

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.

As described in 8.8.1.c, a key benefit of Contact Solutions' 3-way active site architecture is that if an entire data center were to be taken off-line, the platform

would still remain fully protected from a simultaneous outage event at one of the remaining data centers.

8.8.1.e RPO & RTO

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Contact Solutions RPO is 100% and our RTO is within 4 business hours.

8.8.2 Backup and restore service methodologies

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

8.8.2.a Data backups

a. Method of data backups

Contact Solutions' applications record data that describes the usage and performance of each call received or placed. This data is stored online for 2 months then moved to a warehouse structure for 6 months. After the warehouse storage period, the data is moved to tape and retained indefinitely.

Contact Solutions performs daily differential, weekly and monthly full data backups. Data is backed up to a dedicated auto rotation multi-slot robotic library. Contact Solutions utilizes [redacted] data vaulting services for off-site storage.

Data and Source Code

Contact Solutions backs-up and stores its platform data, database data and source code. All Contact Solutions' source code is maintained in a source-safe management configuration system. Platform data and software source code backups are performed and retained according to the following schedule:

Frequency	Backup Type	Retention Period	Site Location
Nightly	Differential	1 week	On-site
Weekly	Full	4 weeks	On-site
Monthly	Full	12 months	Off-site

In addition, exact binary images of TRMs that run the applications are created periodically. These images are stored on DVD media and can be used to replicate or reproduce a specific system as the platform grows and in the event of a single system failure.

8.8.2.b Server image backups

b. Method of server image backups

Contact Solutions' hosted applications are capable of accessing and updating client data located in remote host database systems. The Contact Solutions hardware and

software architecture that supports this functionality is supported within redundant application and database servers.

If any given application or database fails within a single site, a redundant server can pick-up its functionality. Ultimately, customer host transactions are automatically programmed to re-attempt between Contact Solutions sites.

8.8.2.c Digital location of backup storage

c. Digital location of backup storage (secondary storage, tape, etc.)

Exact binary images of TRMs that run the applications are created periodically. These images are stored on DVD media and can be used to replicate or reproduce a specific system as the platform grows and in the event of a single system failure.

8.8.2.d Alternate data center strategies

d. Alternate data center strategies for primary data centers within the continental United States.

The Contact Solutions production platform architecture is designed to ensure business continuity and system redundancy for all our customers' hosted applications. Contact Solutions employs a unique 3-way always-active architecture at the data center level. Three geographically dispersed, continuously linked, yet independently operable data centers automatically and dynamically balance call handling load across all data centers.

Highlights of the architecture include:

- Call allocation across multiple, geographically diverse sites
- Call failover site-to-site
- Customer host transaction interfaces to and from all sites
- Independent application and database servers at each site
- Independent internet and private data network access from each site
- Multiple voice and data network providers at each site

Unique to Contact Solutions, a key benefit of the 3-way active site architecture is the ability to perform routine enhancements and maintenance on the platform without the need for maintenance downtime windows. If an entire data center were to be taken off-line, the platform would still remain fully protected from a simultaneous outage event at one of the remaining data centers.

8.9 Data Protection

8.9.1 Standard encryption technologies

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.

Contact Solutions employs rigorous, documented, implemented, and monitored security standards, which have been and continue to be reviewed as part of a Level 2 SSAE-16 audit and PCI compliance review. We are SSAE-16 certified and PCI and HIPAA compliant.

Data Transmission and Encryption

Contact Solutions has multiple methods to transport data securely:

- Encrypted VPN tunnels
- Private Data Circuit
- Secure HTTP transmission using certificates
    - Latest SSL encryption required for transmission
    - HTTPS is required in the URL
- Secure FTP

Data Storage

Contact Solutions stores non-sensitive client related data locally within the platform database infrastructure. Our platform architecture allows sensitive data to be segmented on physically separate database servers if required.

Additionally, Contact Solutions mandates data masking techniques to ensure that data (i.e. account numbers, SSN, etc.) is stored securely and without manual inspection. Contact Solutions allows for the storage of the first 6 digits or the last 4 digits of sensitive card data, but not full PAN or credit card number. Storage of both within the same application is prohibited.

Contact Solutions prohibits the storage of credit/debit card track data, CVV2 and PIN codes.

Data Encryption Key Management Policy

Contact Solutions IVR and Web services collect, and when required, store customer's sensitive information.

Contact Solutions implements encryption of customer sensitive information by using a two-tiered encryption architecture. Sensitive information is encrypted using a symmetric AES_256 encryption key and stored in a separate database.

The AES_256 encryption key is further encrypted using a certificate generated with the database master encryption key (key-encrypting key). Full password to the

AES_256 encryption key is not known by any one individual and is stored on the database server in an unreadable format. All backup encryption keys are centrally stored on a secure management server.

8.9.2 Willingness to sign agreements with Purchasing Entity

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.

Contact Solutions complies with this requirement. We are willing to sign relevant and applicable Business Associate Agreements or any other agreement that may be necessary to protect data with a Purchasing Entity.

8.9.3 Approved use of data only

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.

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

Please note that Contract Solutions is an experienced government contractor and performs numerous programs that require us to abide by strict limitations on the use of government data. We thus have a proven track record of compliance in terms of standard processes, personnel training, corporate culture, and technology.

8.10 Service Level Agreements

8.10.1 Negotiable SLAs

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.

Contact Solutions complies with this requirement. We will work with individual Purchasing Entities to define agreed upon SLAs. In general Contact Solutions adheres to a 99.999% service level.

8.10.2 Sample SLA

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. .

We have included a sample Service Level Agreement as a separate file entitled Contact Solutions Sample Service Level Addendum.

8.11 Data Disposal

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

Contact Solutions utilizes [redacted] Secure Media Destruction Service for disc and tape destruction. Benefits of the service include:

- Secure transportation of sensitive information
- Trained and rigorously screened personnel
- Accountability with a documented Chain-of-Custody
- An environmentally friendly waste-to-energy incineration process that also ensures complete media destruction

8.12 Performance Measures and Reporting

8.12.1 Guaranteed reliability and uptime

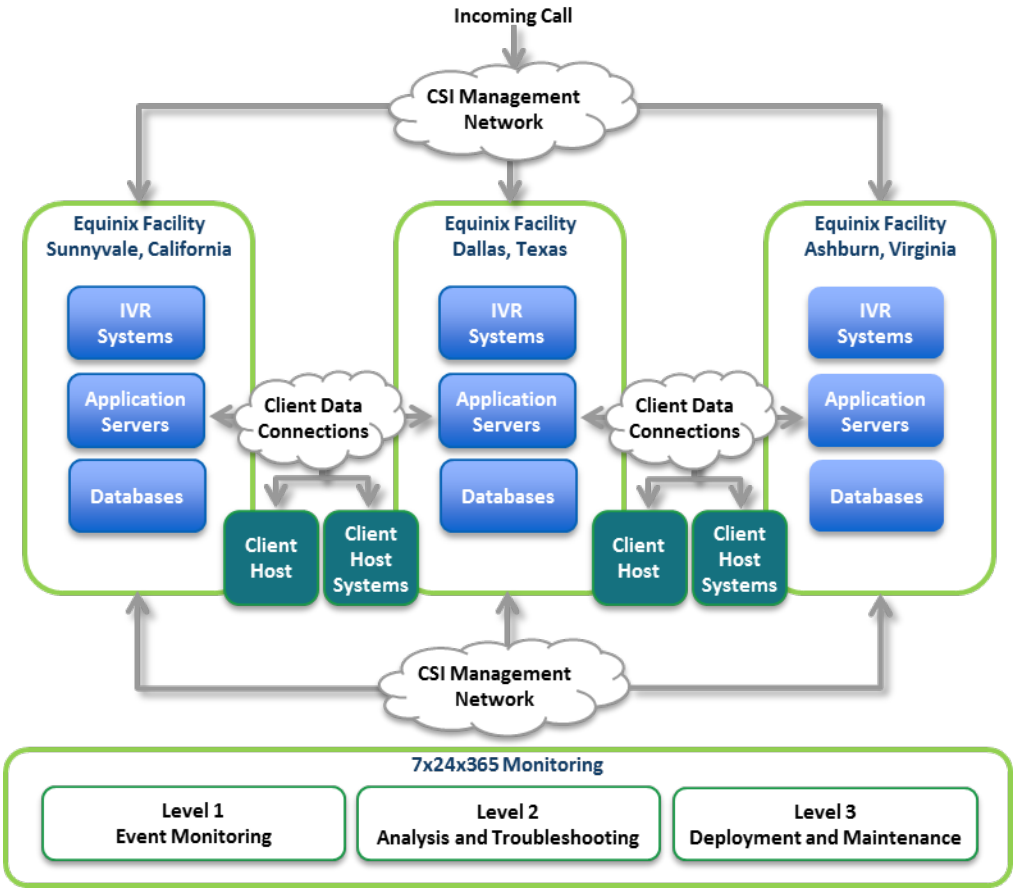
8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

The Contact Solutions production platform architecture is designed to ensure business continuity and system redundancy for all our customers' hosted applications, resulting in an actual availability greater than 99.9%. Contact Solutions employs a unique 3-way always-active architecture at the data center level. Three geographically dispersed, continuously linked, yet independently operable data centers automatically and dynamically balance call-handling load across all data centers.

Highlights of the architecture include:

- Call allocation across multiple, geographically diverse sites
- Call failover site-to-site
- Customer host transaction interfaces to and from all sites
- Independent application and database servers at each site
- Independent internet and private data network access from each site
- Multiple voice and data network providers at each site

Figure 3: Platform Architecture and Guaranteed Reliability and Uptime



Additional fault tolerance features are implemented within each data center, designed to eliminate single points of failure. Computers, servers and network equipment are deployed in an 'N+1' redundant configuration at each layer of the solution architecture.

Unique to Contact Solutions, a key benefit of the 3-way active site architecture is the ability to perform routine enhancements and maintenance on the platform without the need for maintenance downtime windows. If an entire data center were to be taken off-line for maintenance, the platform would still remain fully protected from a simultaneous outage event at one of the remaining data centers.

To ensure that the platform solution remains robust, Contact Solutions performs regular platform performance diagnostic testing to identify and schedule for remediation any identified component weakness. The testing is performed in a 30-minute window in the early morning hours to minimize the impact on system availability. Due to the nature of this testing, availability for individual inbound calls during the test may be impacted but will exceed 99.9% at a minimum. Overall platform availability exclusive of this test time is committed at 99.999%. It is important to note that the data centers have been 100% available since 2004 without interruption.

8.12.2 Uptime service and SLA

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

Contact Solutions understands this Service Level to be representative of up time for the platform. A target of 99.999% is the desired service level. Contact Solutions is able to achieve this service level through the implementation of redundancy and business continuity practices as detailed in 8.12.1.

8.12.3 Support process

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.

Purchasing Entities will have a single point of contact for all questions and issues that may arise during implementation. That point of contact will be the project manager, who will manage development and implementation of the IVR solution, ensuring a full, end-to-end understanding of the intricacies of the Purchasing Entity and the application. The project manager will engage other Contact Solutions resources as necessary.

Post-implementation, Purchasing Entities will have access to our Client Help Desk which provides a dedicated team to respond to requests for application support. This team will be responsible for documenting, escalating (as required), resolving, confirming a satisfactory resolution, and closing all support requests.

Our Engineer on Call (EOC) provides 24 x 7 x 365 support via a centralized pager number. The EOC is available to Purchasing Entities for service-impacting issues outside of normal business hours. Both the Client Help Desk and the EOC have access to all Contact Solutions resources, including the project manager, and will escalate as necessary to resolve the issue.

8.12.4 Remedies for failure to meet incident response SLA

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

Contact Solutions will work with the Purchasing Entity to define consequences/ remedies if incident response/fix time metrics are not met.

8.12.5 Downtime procedures

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

Contact Solutions hosts our applications on a robust platform using common off-the-shelf hardware. The platform is housed in [redacted] hosting facilities located in

Virginia, Texas, and California. This enables us to effectively operate at 100% uptime (our last platform outage was in 2004) with multi-site disaster recovery capabilities. Each site is a 'hot' disaster recovery site, so there is no downtime in shifting traffic between sites as upgrades and maintenance are performed. We load balance all traffic across the three sites to provide 24 x 7 availability and maximum flexibility.

8.12.6 Remedies for failure to meet disaster recovery SLA

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

Contact Solutions will work with the Purchasing Entity to define consequences/ remedies if disaster recovery metrics are not met.

8.12.7 Sample performance reports

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.

Contact Solutions is able to provide both real-time and batch statistics. We will work with the Purchasing Entity to provide performance reports via the Web or in whichever manner bests suits their needs.

We have included a sample performance report as a separate file entitled Contact Solutions Sample Performance Report.

8.12.8 Ability to print reports

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

Contact Solutions complies with this requirement. Authorized Purchasing Entity users have the ability to print historical, statistical, and usage reports locally.

8.12.9 On-demand deployment support coverage

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

Contact Solutions complies with this requirement. Our Engineer on Call (EOC) provides 24 x 7 x 365 support via a centralized pager number. The EOC is available to Purchasing Entities for service-impacting issues outside of normal business hours. The EOC has access to all Contact Solutions resources, including the project manager and will escalate as necessary to resolve the issue.

8.12.10 Scale-up and scale-down

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

Contact Solutions provides a cloud-based IVR for commercial and government clients from a robust, distributed, and highly scalable technology platform. Contact Solutions operates a multi-tenancy, shared resource model hosted IVR system operating across three 7x24x365 data centers. This model maximizes both network efficiency and scalability (including spike capacity) available to all of our clients.

Inbound calls are dynamically allocated in real time across all three Contact Solutions data centers. Any client application can run on any IVR port in any data center, ensuring that each client application has access to the entire pool of available capacity at any moment in time- providing each client with burst capacity that would be costly to replicate in a non-hosted environment. Each client application has access to all of the platform resources within that data center running that application instance as well as access to the redundant resources in other data centers, ensuring that client applications will have access to network resources even in the event of local component failures.

In order to ensure support for unexpected spikes in call volume, Contact Solutions maintains 100% reserve capacity in its active IVR footprint. Our Operations team monitors network utilization and plans system capacity and port availability well in advance of expected volume increases. If utilization begins to exceed 50% of system capacity on a typical day, expansion plans are executed. Forecasting reports linked to our platform automatically notify our purchasing team when it is time to add additional platform capacity. Because we are deployed in [redacted] data facilities and are never constrained by the size of company-owned data centers, there is virtually no limit to our ability to add capacity as required.

Contact Solutions currently averages over 120 million minutes/month on the platform, and maintains reserve capacity capable of absorbing over 120 million minutes/month of traffic spikes across our customer base.

8.13 Cloud Security Alliance

Describe your level disclosure of compliance with CSA Star Registry for each Cloud solutions offered. a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3 b. Completion of Exhibits 1 **and** 2 to Attachment B. c. Completion of a CSA STAR Attestation, Certification, or Assessment. d. Completion CSA STAR Continuous Monitoring.

a. Contact Solutions documents two different types of reports to attest compliance with CSA best practices:
   - Contact Solutions has completed the Consensus Assessments Initiative Questionnaire (CAIQ), which provides industry-accepted ways to document what security controls exist in IaaS, PaaS and SaaS offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer

and cloud auditor may wish to ask of a cloud provider. The CAIQ attachment documents Contact Solutions IVR SaaS compliance.

- Contact Solutions has reviewed the Cloud Controls Matrix (CCM), which provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 14 domains. As a framework, the CSA CCM provides organizations with the needed structure, detail, and clarity relating to information security tailored to the cloud industry. Contact Solutions elects to provide the Contact Solutions - Cloud Controls Matrix Compliance Summary Report, March 9, 2016, which documents Contact Solutions IVR SaaS compliance with Cloud Controls Matrix in the following domains.
    1. Application and Interface Security
    2. Audit Assurance and Compliance
    3. Business Continuity Management
    4. Change Control and Configuration Management
    5. Datacenter Security
    6. Governance and Risk Management
    7. Human Resource
    8. Identity and Access Management
    9. Infrastructure and Virtualization Security
    10. Interoperability and Portability
    11. Mobile Security
    12. Security Incident Management
    13. Supply Chain Management
    14. Threat and Vulnerability Management

b. Contact Solutions has completed The Consensus Assessments Initiative Questionnaire (CAIQ) and the Cloud Controls Matrix (CCM), included as separate files entitled Exhibit 1 to Attachment B_CAIQ and Exhibit 2 to Attachment B_CCM.

c. Contact Solutions provides a completed CSA STAR Attestation, included as a separate file entitled Contact Solutions IVR SaaS - CSA STAR Self-Assessment.

d. Contact Solutions provides a completed CSA STAR Continuous Monitoring, included as a separate file entitled Contact Solutions IVR SaaS - CSA STAR Continuous Monitoring.

8.14 Service Provisioning

8.14.1 Process emergency or rush requests

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

The Contact Solutions Client Help Desk is the main point of contact (POC) for all service issues and application change requests. During the kickoff process for each new application, the Purchasing Entity's project team is provided with a

Troubleshooting and Escalation Standard Operating Procedures document. The key contacts for Contact Solutions and the Purchasing Entity's staff are identified along with the methodology and escalation procedures for reporting a technical issue during normal business hours and after-hours or during holidays.

Many IVR application changes that require immediate attention can be managed by the Purchasing Entity via Contact Solutions' web-based Optimization Portal. Authorized Purchasing Entity staff can modify pre-defined application parameters such as, but not limited to: routing changes, emergency message creation and deployment, call-flow changes, etc. Requests that require Contact Solutions staff are processed through the Client Help desk and escalated as appropriate based on the level of skill and critical nature of the service. Examples of service requests that are not service outage related may include:

- Adding/changing report subscriptions
- Rerunning data feeds
- Optimization Portal access/password creation or resets
- Call trace requests
- Call Detail Records requests
- Application change requests that cannot be addressed via Optimization Portal (e.g. new call flow features/functions, new/modified host integrations, additional network routes, etc.)

Reporting a service-affecting technical issue during normal business hours is documented for the Purchasing Entity's project team using the template, below. Emergency events that occur after-hours or during holidays are directed to Engineer on Call (EOC) staff that is available 24x7x365. The EOC has access to all Contact Solutions resources, and will escalate as necessary to resolve the issue.

Troubleshooting and Escalation SOP Template:

If Purchasing Entity identifies a service impacting incident during normal business hours:

1. Purchasing Entity point of contact shall email or call (email preferred) Contact Solutions Client Helpdesk to open trouble-ticket; copying designated Purchasing Entity distribution list(s). The ticket should contain as much of the following information as possible:
    a. Email Subject Line: Purchasing Entity IVR Production Issue - <APPNAME>
    b. Email Body/Content:
        i. Application(s) affected
        ii. Date & Time of Problem
        iii. Description of Problem
        iv. Details such as ANI, Call Time, Error Message(s)
        v. Impact
        vi. Actions Requested/Taken

2. Contact Solutions point of contact shall acknowledge receipt and provide any additional, relevant information regarding the reported incident and next steps.
3. Contact Solutions point of contact shall remain engaged and provide regular updates through triage, trouble-shooting, escalation and resolution of issue(s).
4. Upon resolution of issue, Contact Solutions point of contact shall ensure Root Cause Analysis (RCA) is published and distributed to appropriate email distribution lists.
    a. If root cause on Contact Solutions' side, then Contact Solutions point of contact shall publish & distribute RCA
    b. If root cause on Purchasing Entity side, then Purchasing Entity POC shall publish & distribute RCA
    c. If root cause undetermined or multiple sources, Contact Solutions point of contact shall ensure RCA is published and distributed as appropriate. For undetermined sources, tracking bugs will be opened to maintain a complete history of the ongoing analysis through resolution.

8.14.2 Lead time for provisioning services

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

The Contact Solutions cloud platform is a SasS-based, multi-tenant environment that does not typically require provisioning platform or network systems to deploy a client solution. The regionally distributed, services oriented architecture of the platform is highly scalable with extra capacity in place to accommodate extreme, and often unplanned, variations in transaction volume found in government programs.

With ready access to available capacity, the lead time for making an application available for access to a Purchasing Agency's constituents is based on the time required to design, develop, test and deploy the application to the platform. The typical timeframe to launch a new application is 60 to 90 days but is very dependent on the nature and complexity of the specific requirements. Contact Solutions' staff will work with each Purchasing Entity to understand their program goals and success criteria as well as any unique requirements of their constituents to customize the self-service solution that meets their specific needs.

8.15 Backup and Disaster Plan

8.15.1 Legal retention periods by agency

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

Contact Solutions complies with this requirement. It is the philosophy of Contact Solutions that all production data-at-rest be retained according to governing state and federal laws, regulatory agencies, and best practices for our industry, including but not limited to the Statement on Auditing Standards No. 70 (SAS70), Statements on Standards for Attestation Engagements No. 16 (SSAE 16), and Payment Card Industry Data Security Standards (PCI DSS). Contact Solutions currently meets the policies and requirements of all of the states and agencies to which we supply IVR services and will continue to do so as a condition of fulfillment of this contract.

The constraints detailed within this policy apply directly to any data-at-rest stored within the Contact Solutions Platform production network. The team responsible for maintaining and implementing this policy is the Contact Solutions Network/Security team. Guidelines on how this policy applies to the different data categories are provided below:

Long-term Data Policy

Long-term data is typically archive data which is to be sent to an off-site storage facility as outlined in other Contact Solutions documentation. This includes items such as database data (e.g. Call Detail Records) and transaction logs. Such data is not to be deleted any sooner than 12 months from the date on which it was created.

Sensitive Customer Data Policy

Sensitive customer data would include any data belonging to our customer which contains information such as PII (Personally Identifiable Information) or credit card PANs (Primary Account Numbers). The only traces of such information on our platform should only be stored in masked or encrypted formats. Discovery of such data anywhere on the network where this is not true must be immediately reported to the Contact Solutions Network/Security team so that the appropriate security mitigation procedures can be initiated. This information must not remain on any platform asset and should be removed as soon as reasonably possible by direction of applicable security protocol.

Short-term Data Policy

Short-term data is typically data that does not get placed into the same media rotation as that of archives and can be disposed of on a case-by-case basis (typically dictated by business and resource drivers). This might include items such as network device configurations or data from platform imaging servers. As an example, an imaging server might contain server images several months old. Such images can be disposed of on an as-needed basis to recover storage space for use by other newer images.

8.15.2 Data recovery risks and mitigation strategies

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

Contact Solutions' applications record data that describes the usage and performance of each call received or placed. This data is stored online for 2 months then moved to a warehouse structure for 6 months. After the warehouse storage period, the data is moved to tape and retained indefinitely.

Contact Solutions performs daily differential, weekly and monthly full data backups. Data is backed up to a dedicated auto rotation multi-slot robotic library. Contact Solutions utilizes [redacted] data vaulting services for off-site storage.

Data and Source Code

Contact Solutions backs-up and stores its platform data, database data and source code. All Contact Solutions' source code is maintained in a source-safe management configuration system. Platform data and software source code backups are performed and retained according to the following schedule:

Frequency	Backup Type	Retention Period	Site Location
Nightly	Differential	1 week	On-site
Weekly	Full	4 weeks	On-site
Monthly	Full	12 months	Off-site

In addition, exact binary images of TRMs that run the applications are created periodically. These images are stored on DVD media and can be used to replicate or reproduce a specific system as the platform grows and in the event of a single system failure.

8.15.3 Multiple data center infrastructure

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

The Contact Solutions production platform architecture is designed to ensure business continuity and system redundancy for all our customers' hosted applications. Contact Solutions employs a unique 3-way always-active architecture at the data center level. Three geographically dispersed, continuously linked, yet independently operable data centers automatically and dynamically balance call handling load across all data centers.

Highlights of the architecture include:

- Call allocation across multiple, geographically diverse sites
- Call failover site-to-site
- Customer host transaction interfaces to and from all sites

- Independent application and database servers at each site
- Independent internet and private data network access from each site
- Multiple voice and data network providers at each site

Additional fault tolerance features are implemented within each data center, designed to eliminate single points of failure. Computers, servers and network equipment are deployed in an 'N+1' redundant configuration at each layer of the solution architecture.

Unique to Contact Solutions, a key benefit of the 3-way active site architecture is the ability to perform routine enhancements and maintenance on the platform without the need for maintenance downtime windows. If an entire data center were to be taken off-line for maintenance, the platform would still remain fully protected from a simultaneous outage event at one of the remaining data centers.

To ensure that the platform solution remains robust, Contact Solutions performs regular platform performance diagnostic testing to identify and schedule for remediation any identified component weakness. The testing is performed in a 30 minute window in the early morning hours to minimize the impact on system availability. Due to the nature of this testing, availability for individual inbound calls during the test may be impacted but will exceed 99.9% at a minimum. Overall platform availability exclusive of this test time is committed at 99.999%. It is important to note that our data centers have been 100% available since 2004 without interruption.

24x7x365 monitoring by the Contact Solutions Network Operations Center (NOC) ensures immediate response to any production level issues that may arise.

We have included our disaster recovery plan as a separate file entitled Contact Solutions Disaster Recovery and Business Continuity Plan.

8.16 Solution Administration

8.16.1 Purchasing Entity to manage accounts

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

Contact Solutions complies with this requirement. We will work with individual Purchasing Entities to define level of access for specific users or groups as required.

8.16.2 Anti-virus protection

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

Contact Solutions complies with this requirement. Anti-virus software with up-to-date virus signatures, real-time scanning, active firewall and URL filtering is

required on all of our systems, including those with access to the Contact Solutions secure environment.

8.16.3 Migrate data to successor

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

Contact Solutions complies with this requirement. We will work with the Purchasing Entity to return call detail record data via a secure server or another method that best meets the Purchasing Entity's needs.

8.16.4 Administer solution in distributed manner

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

The Contact Solutions IVR platform uses a three-tier distributed architecture allowing any one of the three tiers to be upgraded or replaced independently. The user interface is implemented on Windows Servers and uses a standard VXML interface to control interactive media and voice dialogs between humans and computers. The relational database management system on the database server contains the computer data storage logic, business logic, and reporting. The middle tiers run on standard web application servers (e.g. WebLogic, Apache, etc.) and focus on host integrations, reusable code, and business logic.

8.16.5 Apply Participating Entity's policies

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

Contact Solutions complies with this requirement. We will work with the Participating Entity to apply any applicable defined administration policies to our solution.

8.17 Hosting and Provisioning

8.17.1 Documented processes, provisioning stack

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

Contact Solutions documents and maintains detailed documentation on the provisioning, configuration and implementation process for the various solutions offered. System configurations, network provisioning and solutions and monitoring

implementations are maintained and repeatable by being tracked in a SharePoint library using "wiki" concepts.

[redacted]

8.17.2 Tool sets

8.17.2 Provide tool sets at minimum for:

8.17.2.1 Deploying new servers

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)

Contact Solutions utilizes [redacted] to deploy new servers as virtual machines. This tool set ensures consistent and standardized server creation via the use of templates and hardened configurations. Requests for new servers are requisitioned, tracked, approved, and provisioned according to specification with ease and speed.

8.17.2.2 Creating and storing server images

2. Creating and storing server images for future multiple deployments

Contact Solutions standardizes server builds by classifying server types and building hardened templates that are then stored separately from production systems. These server templates are managed and maintained with updates and patches, and have version control management implemented.

8.17.2.3 Securing additional storage space

3. Securing additional storage space

Storage is managed and tracked using both a common management tool set [redacted] as well as the vendor's proprietary storage tools. Storage capacity is tracked at the raw disk level, as well as by volume and by drive. Being virtualized, storage can be procured and added as needed, where needed, with flexibility for different performance tiers of storage used as needed.

8.17.2.4 Monitoring tools

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).

Contact Solutions provides a complete monitored solution for customers using our own internal Network Operations Center (NOC). The NOC monitors the cloud components and services on a 24x7x365 and provides custom-tailored alerts to issues or service degradation directly to the customer, allowing for personalized notification and escalation. While the NOC uses several different tools, two systems are highlighted below.

[redacted] provides in-depth analytical data in both real time and historical fashion. This data can be used to provide configuration, performance, inventory and raw data from the hosts to the Virtual Machines, and to also provide business views that allow detailed trending and analysis.

[redacted] Multi-vendor network monitoring software for fault, performance and availability monitoring. This tool monitors our applications in public, private and hybrid cloud environments and provides Management Dashboards.

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

8.18.1 Testing and training periods

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

All implementations and system modifications go through a comprehensive testing and acceptance protocol. The testing cycle includes several stages. During all testing activities Contact Solutions prohibits the use of live production data for testing and development.

Once the test plan is created and the solution is ready for test, the following test cycles are applied:

- Test Prep: The overall test plan and individual test cases are created; test and UAT environments are set up and configured.
- Unit Testing: The development team tests the application, creates bugs that represent typical issues, and then retests until all issues are resolved.
- Development Integration Testing: The Integration Test team performs integration testing to ensure all data connectivity and host integrations are working properly.
- System Testing: The System Testing cycle, coordinated by the project manager, includes full application and integration testing, testing of failure conditions,

testing of secure communications, validation of input and output, and encryption and data masking when appropriate.

- User Acceptance Testing: Once the internal QA process is complete, the application is deployed to the User Acceptance Testing environment. During this phase, the Purchasing Entity vigorously tests the application and reports any issues.
- Regression Testing: Upon the resolution of any issues found during testing, the application is then regression tested with the new fixes to ensure the strength of the overall system. Once the application is tested by the Purchasing Entity, a formal sign off is completed.
- Production Integration Testing: The project team works with the Purchasing Entity to ensure that all production data connectivity and host integrations will work in the production environment.

We work with the Purchasing Entity to develop a training plan that suits their specific IVR program and the degree to which agency administrators will need to use the Optimization Portal to effect changes. These factors will determine the amount of training needed, which will be scheduled to occur and be finished between acceptance testing and the go-live date.

8.18.2 Test environment

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

Contact Solutions' standard practice for delivering a solution includes a User Acceptance Period that meets the Purchasing Entity's specific requirements. The Purchasing Entity is provided with a test environment that replicates the production environment including access to a test host environment so complete end-to-end testing can be performed.

[redacted] Web Vulnerability Scanner is used for all new and modified web application code to ensure OWASP compliance. These scans check for cross-site scripting, SQL injection, malicious file execution, information leakage and error handling, and authentication and session management. No code will be released to production until it is deemed PCI compliant.

[redacted] is used to test performance on both static and dynamic application resources. The tool simulates a heavy load on application components to test its strength and to analyze overall performance under load.

8.18.3 Training and support, no additional cost

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

As Contact Solutions is providing a fully managed solution, the training requirements will be minimal. Training will be handled through one-on-one mentoring and covers how to utilize the reporting portal as well as the Contact Solutions Optimization Portal, which allows authorized Purchasing Entity staff to make changes to their application parameters and call routing. Contact Solutions staff will remain available to the Purchasing Entity throughout the term of the contract to provide any additional training as required. In most cases, training is done using remote training tools via web-conferences.

Purchasing Entities will have a single point of contact for all questions and issues that may arise during implementation. That point of contact will be the project manager, who will manage development and implementation of the IVR solution, ensuring a full, end-to-end understanding of the intricacies of the Purchasing Entity and the application. The project manager will engage other Contact Solutions resources as necessary.

Post-implementation, Purchasing Entities will have access to our Client Help Desk which provides a dedicated team to respond to requests for application support. This team will be responsible for documenting, escalating (as required), resolving, confirming a satisfactory resolution, and closing all support requests.

Our Engineer on Call (EOC) provides 24 x 7 x 365 support via a centralized pager number. The EOC is available to Purchasing Entities for service-impacting issues outside of normal business hours. Both the Client Help Desk and the EOC have access to all Contact Solutions resources, including the project manager, and will escalate as necessary to resolve the issue.

8.19 Integration and Customization

8.19.1 Integrating the solution with complementary applications

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

As a hosted IVR service provider, Contact Solutions designs, develops and maintains many varied end-to-end integrations. Protocols supported range from web enabled services to traditional 3270 screen scraping. Web Services, HTTP, HTTPS, SOAP, XML, CORBA, MQ Series, Sybase OC, RPC, JDBC, ODBC are some examples of current implementations. LAN/WAN access can be via public or private networks utilizing Internet, VPN, Frame, ISDN and other network capabilities.

The automation system needs to be built with gateway services that integrate with each system. The gateways should be built so all communication modes (e.g. IVR, text messaging, mobile, etc.) can access the data without requiring a new gateway

service to be built for each medium. By building a common gateway service as a mediation layer between the medium and the data, Purchasing Entities and agencies will have the flexibility to offer services that meet the needs of the community with minimal additional development cost.

Another aspect of integration that needs to be considered is the establishment of the secure connections used to interface with the host systems. During this activity, the circuits are provisioned (which include ordering, receiving, configuring, and testing the circuits). Contact Solutions will work with the Purchasing Entity on connectivity tests to ensure and document the interfaces are working properly and able to transfer data accurately and completely.

8.19.2 Customizing and Personalizing the Solution

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

Contact Solutions provides a comprehensive packaged IVR application based on the lessons learned from billions of calls. The application is highly configurable and customizable such that configurations changes can be made in real-time via a web portal. Additionally, the application can easily be customized to suit Purchasing Entity needs. The lead time for personalized application changes is dependent on the scope of the changes required.

Based on data collected from more than 12 years of caller interactions, Contact Solutions has established best practices for IVR applications. Before any engagement with the Purchasing Entity begins, a Project Manager is assigned and is responsible for managing and coordinating all facets of the solution development process from initiation through completion.

Planning and Administration

A kick-off meeting is scheduled in order to introduce all the key participants in the project, to open the lines of communication between all members of the project team on both the Purchasing Entity and development sides, and to clarify the general high level IVR system functionality and requirements. Upon agreement with the Purchasing Entity regarding the high level design and required features of the solution, a detailed analysis to define requirements is conducted. All the appropriate personnel are leveraged to support the project. During this phase, all regular status meetings are scheduled for the duration of the project.

Define Requirements

During this phase of the project, the detailed requirements are defined by the Purchasing Entity and our project team. Once the requirements have been agreed upon, a written assessment is provided for official sign off prior to beginning development. The Purchasing Entity's reporting requirements are defined and documented as well. Additionally, the necessary data integration and telecom requirements for the project are determined, and the team begins the coordination

of enabling these components at this time. All of this information is included in a published Business Requirements Document (BRD) and provided to the Purchasing Entity for approval.

Design Solution

Once the BRD has been agreed to and approved, the design team will engage in creating a draft call flow for the solution, using the BRD and Purchasing Entity scripts as fundamental elements. A call flow is a graphic representation of the entire solution, showing all the elements call progress and reporting process, as well as all the detailed data integration necessary at different points in a call to the solution. Other key components included in the BRD and call flow include:

- Message Prompts: All of the final prompt messages to be used by the solution will be documented and approved. Contact Solutions engages a professional voice talent to record the spoken messages and will create any necessary fax and email templates to be delivered to the Purchasing Entity's constituents.
- Data Integration: This task encompasses the creation of the data transfers that will deliver customer files from client databases to the IVR system for transmission to the Purchasing Entity's constituents. During this phase, data circuits will be ordered, provisioned, tested and made live.

The call flow, combined with the BRD, will serve as the design template throughout the development process. As requirements or design changes occur, change orders are processed and approved; these documents are then updated and redistributed to all the project stakeholders.

Development and Delivery

Our IVR delivery process is a modified software development life cycle process. Voice User Interface (VUI) design, usability and tuning are unique, but can be likened to the process used to develop web applications. VUI design focuses on the customer experience (i.e. human factors).

Our design team works with a statistically relevant sample of potential IVR users and studies their interaction with the application to ensure optimum usability. We focus on likely IVR scenarios to ensure the users can complete the expected task within the VUI.

Development occurs within the Integrated Development Environment (IDE). Testing is performed both within the IDE and on the platform test ports.

Integration ensures that all the hosted and Purchasing Entity side components are available for the developed application and are ready for launch.

Deployment

In the Deployment Phase, we deploy the IVR application to the production ports and resources and move the volume to the application.

We continuously tune the solutions, focusing on how real life constituents are interacting with the IVR application. The users' experience and results are statistically studied.

Support consists of monitoring the application and includes evolutionary changes to the application as requirements grow and business purpose changes. During the support activities, we repeat some or all of the previous steps dependent on the scope of the change.

8.20 Marketing Plan

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

Contact Solutions is focused almost exclusively on marketing and selling to states and large municipalities. Our past experiences with large state contracts have given us a unique perspective on how to identify agencies that sponsor citizen interaction programs with unmet potential for automation through self-service IVR. We have developed an approach for educating those agencies on how such services can best be implemented to meet their specific requirements, and what levels of cost savings and efficiencies can be achieved. Our methodology revolves around a few key activities we perform regularly.

Contact Solutions will implement the NASPO recommended marketing model as well as our expertise in working with and marketing to state agencies and identifying state contract opportunities. Contact Solutions will determine the best methods in regards to the NASPO participating state members, as well as individual procurement opportunities in our outbound and inbound approaches.

Example marketing and identification activities include:

- Development of NASPO customer information and promotional materials
- Development and promotion of NASPO website page, including links to MA, PAs
- State education and information through datasheets, blog posts, and case studies
    - Market to state Cooperative Purchasing Organizations (CPO), staffers and other agency contacts
    - Market to state agencies and political subdivisions alerting them of this new contract and simplicity of purchasing
- Engage and cooperate with Lead State, NASPO ValuePoint, CPOs
    - Monitoring of participating states' contracts and procurement processes (state agencies, Deltek, CPO)
    - Attend and participate in pre-bid and bid meetings and vendor process

- Participation in various state marketing activities and events with organizations such
    - e-Republic Digital Government
    - EFTA eGovernment Payments Council
    - NASTD
    - NASCIO
    - APHSA
- Additional promotion of participation in NASPO ValuePoint Contract
    - Table top displays
    - Presentations
    - Datasheets
    - Emails
    - Giveaways
    - Social media (Twitter, LinkedIn)
- Ongoing relationship and value development – over time leverage ValuePoint Contract awards and contract results to gain state references, recommendations, and referrals

Our marketing team takes an inbound approach to drive lead generation. Inbound marketing relies on high volume and high quality content generated and posted on our website and through social media. The purpose of this activity is to make valuable information available to state employees when they need it and want it for the programs they are pursuing, which ends up leading them to Contact Solutions. For NASPO and for the states participating in this RFP, Contact Solutions will continue to generate and post pertinent information about the contact center programs we have implemented across more than 40 states and agencies.

Once we have been awarded this contract, Contact Solutions marketing will post the information about the contract on our website. We will also provide Twitter and LinkedIn feeds from our Contact Solutions accounts as well as providing them for our employees to post on their own accounts. Links to the NASPO website, to the Master Agreement and to the States with Participating Addendums will also be included.

8.21 Related Value-Added Services to Cloud Solutions

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

Contact Solutions' usage-based value proposition ensures that we maintain our commitment to automating more calls tomorrow than we do today while improving the overall experience for the Purchasing Entity's constituents. Through our ability to offer more effective self-service, we are able to guarantee savings, not only on deployment, but throughout the course of the relationship.

Our Best Practices and Analytics Teams are responsible for our Continuous Improvement (CI), Customer Experience (CX) and Business Intelligence (BI) programs. Their overall goal is to ensure our designs are completed using the best practices developed over the last 12 years, provide the reporting and analytical tools necessary to fine-tune production systems and complete ongoing application analyses to ensure a high level of customer experience as callers complete their journey through our applications.

Continuous Improvement

Contact Solutions ensures IVR performance is always optimized to current contact center processes, business goals, and customer experience initiatives. Thanks to our embedded culture of CI, and more specifically, our dedicated CI Practice, Contact Solutions has the proven measurements, as well as the expertise and experience to use these analytics to drive improvements in your solution's performance for the life of our relationship. Our CI Practice saves our clients over $15M annually.

With Contact Solutions, Purchasing Entities will improve performance, not just at initial implementation, but throughout the life of our relationship. Our approach is deeply tied to data and analytics. Monitoring the right KPIs is important, and we do that. Continually measuring and analyzing those KPIs to drive data-based decisions is paramount to maximizing performance. Without a strict process to measure the right data, and then not just make it actionable, but take action, many leave performance improvements—and millions of dollars in cost savings—on the table.

Our CI Practice invests time to gain a deep understanding of our clients' strategic objectives and then, by measuring and analyzing call data and performance metrics, recommends enhancements - including, but not limited to, menu structure, self-service improvements, call flow improvements, speech tuning, and CTI changes. These enhancements improve contact automation and overall Customer Experience. We deliver solutions that leverage proven processes and patented technologies that improve the customer experience while reducing operational costs, again and again – not just at initial implementation.

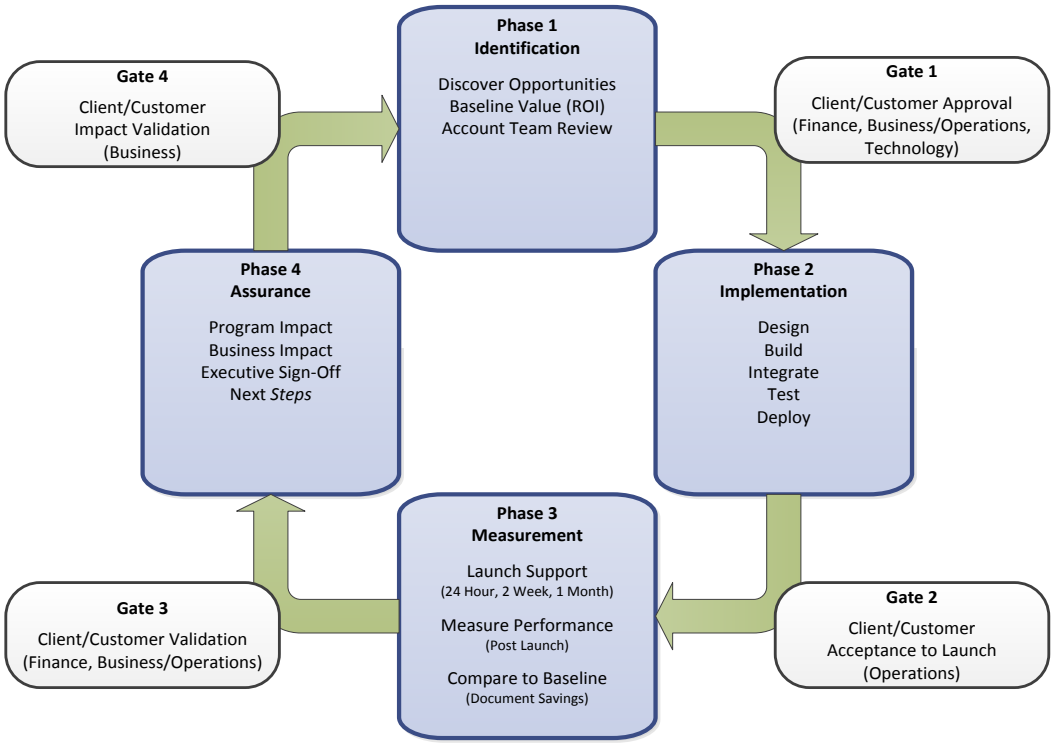
The CI Team has developed and refined a repeatable four-phase Continuous Improvement methodology that provides life-cycle management of IVR applications while ensuring alignment with Purchasing Entities and their customer experience goals. These four distinct phases include:

- Identification: Benchmarking existing performance, identifying CI opportunities, and estimating benefits (in savings and CX improvements) are key components of the identification phase. This process allows our experts to understand Purchasing Entities' business practices, processes, environment, constituent perspective and challenges. We use a set of

established discovery tools to gather information and data. An experienced CI Analyst uses these findings combined with our comprehensive reporting capabilities to establish specific improvement targets related to self-service, CX, transfers to agents and dollar savings associated with each.

- Implementation: This phase begins after Purchasing Entity approval of recommendations and includes system design, development, testing and implementation. Our discovery process ensures we develop a clear understanding of callers' needs. This allows us to apply our user-centered design process to match a Purchasing Entity's business goals with those needs. We leverage existing enterprise user-centered strategies to improve time-to-market, minimize risk, and increase caller adoption of self-service.
- Measurement: Actual, post-implementation KPIs (self-service rate, automation rate, CX score) are compared against the measured baseline. These results are then reviewed with the call center management team, savings are calculated, and a summary package of the Continuous Improvement changes prepared.
- Assurance: The package is reviewed with executive sponsors for final sign off.

Figure 4: Contact Solutions Continuous Improvement Process



Customer Experience

Contact Solutions developed a process for measuring Customer Experience Rating (CXR) within the IVR and mobile customer support applications. This process uses a set of behavior metrics and a scoring framework to document a caller's journey. Contact Solutions' CXR process was awarded the Frost and Sullivan Product Differentiation Award in 2013 for its unique and valuable approach to CX management.

The CXR report captures and reports on eight key metrics that reflect customers' experience interacting with the automated applications. By analyzing these metrics and trends over time, we are able to make recommendations on how to improve our customers' experiences within each application and predict – with accuracy – their impacts. The eight customer experience elements include:

- Continuity: A measurement of an application's ability to transfer customer information and intent across all channels.
- Notification: Measures the use and success rate of the notification systems employed in proactively delivering information. These systems include SMS, outbound IVRs, and email solutions.
- Data Access: Measures the success and accuracy of an enterprise's information gateway as the point of access for all customer information.
- Personalization: An application's ability to modify the caller experience based on user interactions, known intentions and established business rules within a single call and across multiple calls.
- Goal Completion: Measures the caller's intent (reason for calling), the interactions or tasks needed to accomplish that goal and the overall success in achieving the goal.
- Navigation: Measures the ease or difficulty in progressing from one interaction point to the other within an application call flow.
- Success Factor: Measures the caller's disposition/satisfaction at the end of each contact with an automated application.
- Authentication: Measures a caller's success in confirming their identity in the automated system.

Business Intelligence

Our solutions rely on business intelligence at the core to improve and personalize Customer Experience (CX) and drive better operational performance, while having the ability to manage the risk of fraud. Contact Solutions can help states and agencies offer effortless care – in both self-service and live agent interactions – at a sustainable cost while adapting quickly to rapidly changing constituent demands.

Constituent contact center interactions, especially self-service transactions, generate massive amounts of data that can help meet constituent needs and navigate the risks of fraud—but only if access to the data is easily and effectively delivered to meet a Purchasing Entity's flexible needs. Contact Solutions' Business Intelligence (BI) Gateway is a cloud-based analytics tool that offers greater visibility to customer self-service intelligence across interactions, helping Purchasing Entities

more effectively and accurately monitor performance, assess and improve CX, and identify cost savings opportunities.

Our solution enables a view and understanding of constituent activity, preferences, and program metrics within a specific program, and across multiple programs, to help the states and agencies better meet the needs of their constituents.

- Precise reporting and analytics
- Complements existing data tools to better serve your customers
- Flexible, dimensional data that can be "sliced and diced"
- Ability to create your own reports
- Convenient access
- Deeper understanding of constituent intent, behavior, and experience

Our customers benefit from instant access and insights into a Dashboard and Reports views of constituent interactions at a high-level view with drill-down options. These actionable, easy-to-read standard dashboards are available on-demand and provide instant access to meaningful customer success data to improve your interaction strategies.

- HostTrak: Displays host interface performance data
- IVR Exit Points: Identifies where callers exited self-service; can identify areas in need of attention
- IVR Call Volume: Presents detailed view of call and minute volume, total transfers, and transfer percentages
- Personalization: Details customer behavior for Adaptive Personalization users to improve CX

8.22 Supporting Infrastructure

8.22.1 Purchasing Entity's infrastructure

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

As a hosted IVR service provider, Contact Solutions designs, develops and maintains many varied end-to-end integrations for our clients. As required, Purchasing Entities will need to provide access to integrate with customer information.

IVR applications running on the Contact Solutions hosting platforms can integrate locally or remotely with Purchasing Entity data. These integrations are accomplished via secure transmission over the public Internet or private data networks.

Data transmitted across a VPN are encrypted using standard IPSEC 3DES or AES-256 encryption. All private point-to-point frame and MPLS integrations come through a DMZ. Network segmentation by client within the Contact Solutions DMZ is accomplished using VLAN configuration.

Client connections via the public Internet are implemented across a VPN or use secure HTTP. In some instances, client data is transmitted and received in a batch configuration via secure FTP.

Contact Solutions will work with the Purchasing Entity on connectivity tests to ensure and document the interfaces are working properly and able to transfer data accurately and completely.

8.22.2 Responsibility for new infrastructure

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

Contact Solutions will provide and maintain responsibility for all equipment, software and network infrastructure required to deliver the cloud-based services up to the Purchasing Entity's network demarcation point. Any modifications to the Purchasing Entity's host systems telecommunication or network infrastructure that may be required to accommodate telephony or data access are the responsibility of the Purchasing Entity.

8.23 Alignment of Cloud Computing Reference Architecture

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

Contact Solutions' Interactive Voice Response (IVR) product offers a Software as a Service (SaaS) solution via private cloud, which is fully compliant with NIST Special Publication 800-145, The NIST Definition of Cloud Computing. The solution meets all five essential characteristics, is a SaaS service model, and the deployment model is private cloud.

The Enterprise Architecture of the IVR SaaS is designed to be tolerant of network failures and bandwidth inconsistency. The interoperability capability of the solution ensures disparate services, including the clients' enterprise, can seamlessly interact.

The IVR capability provided to the client is a bundled solution that encompasses all three domain layers; IaaS, PaaS, and SaaS. The SaaS is fully managed; client does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage. Individual application capabilities, limited to user-specific application configuration settings, are accessible from various client devices through a web browser. The IVR SaaS can be interfaced to connect directly to the clients' information systems to drive response, collect data, or support other client requirements.

Confidential, Protected, or Proprietary Information

In accordance with the RFP requirements, Contact Solutions has completed a Claim of Business Confidentiality form provided as separate file entitled Contact Solutions Claim of Business Confidentiality.

6.1 Business Profile

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

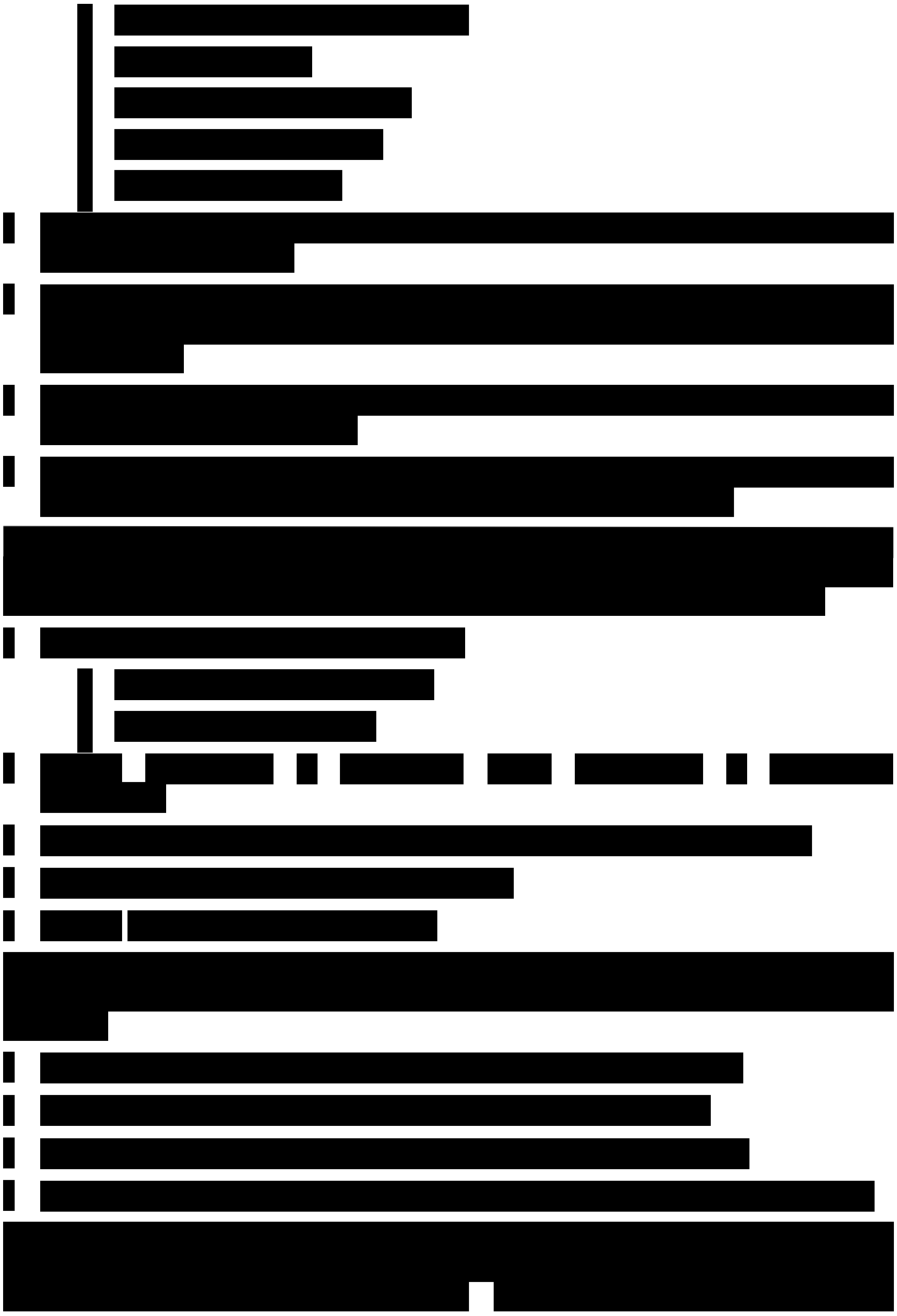
[redacted]

6.2 Scope of Experience

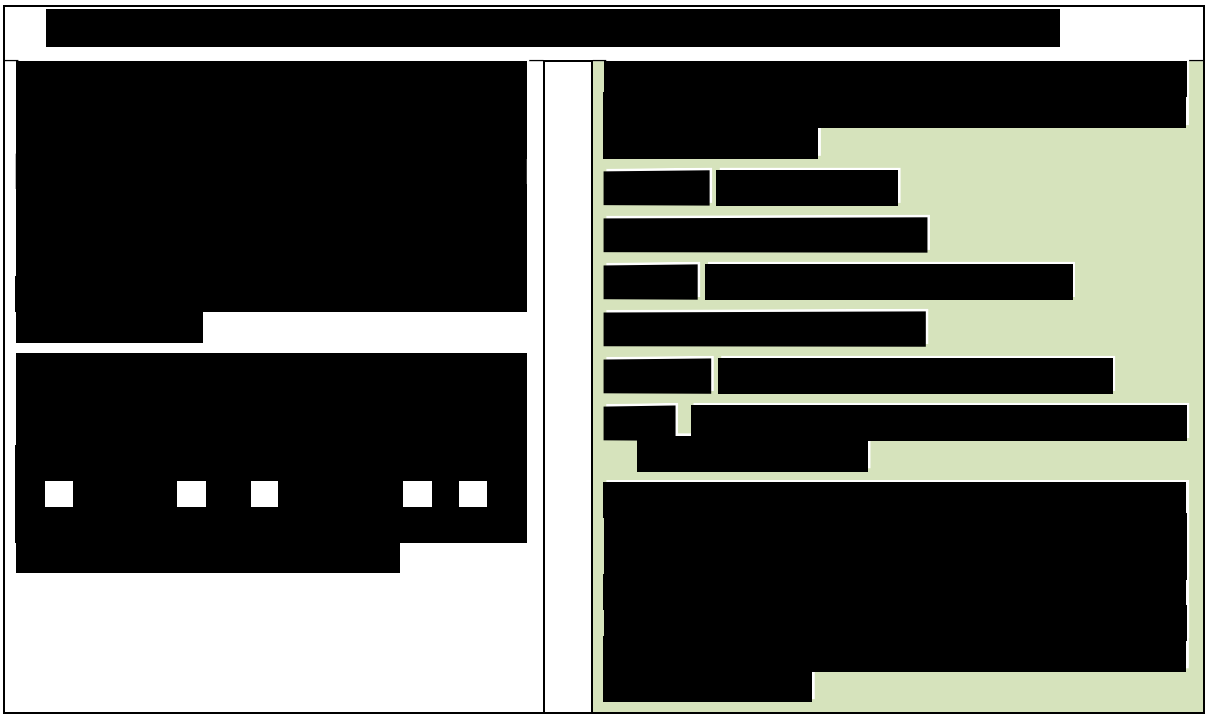
Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the business provided offerings identical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

[redacted]

[redacted]



[redacted]



6.3 Financials

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

[redacted]

[redacted]

7.1 Contract Manager

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

[redacted]

7.1.1 Contract Manager contact information, work hours

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

[redacted]

7.1.2 Contract Manager experience, resume

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

[redacted]

ATTACHMENT E

NASPO ValuePoint - INTELLECTUAL PROPERTY ATTACHMENT

(a) Customer acknowledges that CS develops or licenses software applications, workflow templates and scripts for a variety of platforms and environments. Except for the rights expressly granted herein, CS hereby retains all right, title and interest in and to: (i) all operating applications, workflow templates and scripts and enabling software, hardware and technology used in connection with the provision of the Services, and all inventions, copyrights, trade secrets, know-how, tools, tips or tricks, utilities, methodologies, trademarks and other intellectual property and other proprietary rights and interests developed or employed by or on behalf of CS in performing Services hereunder that were used by CS prior to or independently from the performance of those Services for Customer, or that are applicable or may be generally useful in performing Services to other CS customers (the "**CS Technology**") and (ii) the application software embodying the Customer workflows (apart from workflow templates) and logic specifically developed for Customer by CS for use with the CS Technology and made available in connection with the provision of the Services and all related documentation, excluding and apart from any CS Technology ("**Custom Application Software**"). Subject to Customer's compliance with the terms and conditions of this Agreement, CS hereby grants Customer a non-exclusive, non-transferable, non-sublicenseable license to access the features and functions of the CS Technology made available in the Hosting Services during the Term for Customer's internal business purposes solely in accordance with this Agreement and any access protocols or other written instructions provided by CS. Notwithstanding anything in this Agreement or any SOW or any other writing relating to and made a part of this Agreement, nothing herein shall limit or transfer in any way CS's ownership or right to use the CS Technology or require CS to deliver to Customer a copy of the CS Technology or Custom Application Software or any component thereof. In addition, Customer acknowledges and agrees that CS may perform services similar to the Services for third parties and in doing so may use the same personnel and CS Technology used in performing the Services for Customer. Each party acknowledges and agrees that the CS Technology includes certain software products licensed to CS by third party software providers (the "**Third Party Software**"). All rights in the CS Technology and the Custom Application Software not expressly granted herein are reserved to CS.

(b) Subject to Customer's compliance with the terms and conditions of this Agreement, CS hereby grants Customer an exclusive, non-transferable, non-sublicenseable, worldwide, fully paid, royalty free license to access, reproduce and use the Custom Application Software solely for Customer's internal business purposes. In addition, after the termination of this Agreement, Customer may allow a third party service provider, subject to Section 6(a)(iv), to install, use, execute and reproduce the Custom Application Software on Customer's behalf solely in connection with its provision of services to Customer. CS will not use the Custom Application Software for any third party.

(c) Customer shall own the Customer Content. "**Customer Content**" means all data, media, information and content provided by Customer or its users for use with

the Services, including the Scripts and information provided by callers of Customer. Customer hereby grants to CS a non-exclusive, non-transferable right and license to: (a) use the Customer Content during the Term for the limited purposes of performing CS's rights and obligations under this Agreement and (b) on a perpetual basis, (i) use, display, modify and create derivative works of the Customer Content solely to derive, create and compile aggregated statistics and/or data that is not personally attributable to or identified with Customer or any individual Customer caller ("**Aggregate Data**"); and (ii) copy, display, disclose, modify and distribute the Aggregate Data. Notwithstanding anything in this Agreement, CS may, without liability or obligation, utilize its or its suppliers' database to confirm caller name, address and telephone number and may update and supplement such database with name, address and telephone number obtained as a result of providing the Services. Customer will have no express or implied right to license CS's database or otherwise have any right to or in CS's proprietary or licensed data.

(d) Without limiting the foregoing, CS may utilize data capture, syndication, and analysis tools, and other similar tools, to extract, compile, synthesize, and analyze Transactional Data. "**Transactional Data**" means any non-personally identifiable data or information resulting from a caller's use of the Services (e.g., the number of callers that press "1"). To the extent that any Transactional Data is collected by CS, such Transactional Data will be solely owned by CS and may be used by CS for any lawful purpose, provided that the Transactional Data is used only in an anonymized and aggregated form and in a manner that does not permit the identification of Customer or any individual caller. CS agrees to comply with applicable privacy and other laws and regulations respecting the dissemination and use of such Transactional Data.

(e) Customer will not (i) copy or duplicate the Services or CS Technology except as explicitly authorized in this Agreement; (ii) decompile, disassemble, reverse engineer or otherwise attempt to obtain or perceive the source code from which any software component of the Services are compiled or interpreted; (iii) modify the Services or the CS Technology, or create any derivative product from any of the foregoing, except with the prior written consent of CS; or (iv) assign, sublicense, sell, resell, lease, rent or otherwise transfer or convey, or pledge as security or otherwise encumber, Customer's rights under this Agreement. Customer will ensure that its use of the Services, the CS Technology and all Customer Content complies with all applicable federal, state or local laws, statutes, regulations or rules. Customer shall notify CS immediately of any unauthorized use or any other known or suspected breach of security in connection with the Services. Customer represents, warrants and agrees that the Customer Content and its use in the interactive voice response system operated by CS or with the Services will not infringe any third party's copyrights, trademarks, trade secrets, patents, or other proprietary rights.

CONTACT SOLUTIONS, LLC
STATEMENT OF WORK/TASK ORDER #__

This Statement of Work (the "**SOW**") is made and entered into on _____ ___, 20__ (the "**Effective Date**"), by and between **Contact Solutions, LLC**, with offices at 11950 Democracy Drive, Suite 250, Reston, Virginia 20190 ("**CS**"), and _____, with offices at _____ ("**Customer**"), pursuant to that certain Master Services Agreement (the "**Agreement**") dated _____ ___, 201_ by and between CS and NASPO ValuePoint, to which it is attached and incorporated. In the event of any conflict between the terms and conditions of this SOW and the terms of the Agreement, the terms of this SOW shall prevail. Except as set forth below, all terms and conditions of the Agreement shall remain in full force and effect. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. **TERM.** The term of this SOW will commence on the Effective Date hereof and will continue until all Services herein are completed, unless earlier terminated as provided in the Agreement. Upon any termination of this SOW, (i) Customer will immediately discontinue all use of the SOW-specific Services and CS Technology and return to CS any copies thereof; (ii) each party will delete any SOW-specific Confidential Information of the other in its possession or under its control; and (iii) CS will delete any SOW-specific Customer Content in its possession or under its control.

2. **SERVICES.** This SOW describes the scope, responsibilities, deliverables and milestones associated with delivering a contact automation solution for the _____ application (the "**Application**"). CS will provide to Customer the following Services:

(a) Hosting Services:
[To be completed by CS and Customer]

(b) Professional Services:

(i) Deliverables and Specifications:

[To be completed by CS and Customer]

(ii) Roles and Responsibilities:

Project Management

When this SOW is executed CS will assign a Project Manager who will coordinate with the Customer in determining a project start date as well as a go-live date. CS will provide the following management-related functions during the development and deployment of the Deliverables as applicable:

(a) Weekly status reports regarding Milestones and Deliverables
(b) Consultation to Customer regarding optimal testing, deployment procedures, and use of the Deliverables in the Customer's or the Customer's end customer environment

Design

CS will be responsible for the following during the design phase:

(a) Development of the user interface specification (call flow), representing the user interface to be presented to callers in order to meet the requirements as specified in the requirements specification document. The call flow will be drafted by CS (using MS Visio) for review and approval by Customer, and may be thereafter modified by CS, at Customer's request, in a manner that does not conflict with the requirements specification document.
(b) Develop a network systems architecture and data integration plan to include any Customer business systems used by the application as necessary.

Development

CS will be responsible for the following as applicable after the design has been signed off, data connectivity transaction testing has been successfully achieved:

(a) IVR application software development
(b) Back-end integration and development
(c) Direction of voice talent
(d) Application integration
(e) Quality assurance

(iii) Milestones, Deliverables and Completion Dates

[To be completed by CS and Customer]

(c) Service Levels. The applicable terms of the Service Level Agreement contained within the Master Agreement will apply to the performance of Services hereunder.

Nothing in this SOW will require CS to perform any Services in violation of any Laws, as determined by CS in its reasonable discretion and CS will notify Customer immediately. If CS believes that its Services cannot be performed as described in this SOW without violating or aiding or abetting the violation of a Law, CS may, in addition to its other rights under this SOW and the Agreement, terminate the Services immediately by notice to Customer. Such termination will not be deemed a breach of the Agreement or this SOW, and CS will not incur any penalty or financial obligation of any type or kind as a result of such termination.

3. CUSTOMER RESPONSIBILITIES.
[Add any SOW-specific responsibilities here.]

[Add any Customer expenses here. Travel etc. is included in the MSA.]

4. ACCEPTANCE.

[To be completed by CS and Customer and as defined in the Agreement]

****

Acknowledged and agreed to by a duly authorized representative of the respective parties.

AGREED:

_____	**CONTACT SOLUTIONS, LLC**
By: _____	By: _____
Name: _____	Bridget Lange
Title: _____	VP, Finance & Administration
Address: _____	Address: 11950 Democracy Drive, Suite 250
_____	Reston, Virginia 20190
_____	
Attn: _____	Attn: Finance Department
Billing Number: _____	Billing Number: (703) 745-5585
Facsimile: _____	Facsimile: (703) 480-1676

SERVICE LEVEL ADDENDUM

Performance Standards

Service Element	Measure of Service Level (SLA) On Monthly Basis	Monthly Credit
Platform Availability	1. The platform supporting CS contact automation software applications ("**Applications**" and each, an "**Application**") will be available to the Customer to accept user traffic **99.999%** of the time, measured monthly with the exception of the following, which shall not be included in determining whether this SLA has been met: a) In the event that the availability of Customer's Application platform is temporarily interrupted by an emergency, CS will provide notice to the Customer point-of-contact within 30 minutes of discovery of the service interruption by CS. b) Once each month, CS performs regular diagnostic testing of platform performance during a 30 minute window in early morning hours (ET). User traffic may be impacted by such testing, but availability will meet or exceed 99.9% during each such test window.	For each tenth of a percent (.1%) below the availability of the System defined in Section 1, a **$500 credit** shall be applied.
Platform Reliability	2. The performance of CS's systems will meet the following service levels:	For each tenth of a percent (.1%) below the performance standard defined in Section 2, a **$250 credit** shall be applied.
Host Processing Availability	a) "**Host Processing Availability**" is defined as the portion of the host process under the control of CS that relies upon Customer's system availability, and will be **99.5**%. Any failure to achieve this SLA that is related to Customer's host responsibilities shall not be included in the monthly calculation of such SLA.	
Application Performance	b) The Application(s) will respond to **99.5%** of user prompts within an average of one (1) second, measured on a monthly basis, provided that any failure to meet this standard that occurs (i) beyond the control of CS or is related to Customer's host responsibilities or (ii) because of any delay caused by complex data (including without limitation large vocabulary or natural language speech) shall not be included in determining whether this standard has been met.	
Standard Call Detailed Reports	3. Standard call detailed reports shall be delivered and made available via Web access for the previous reporting day. Weekly reports shall include calls from Sunday through Saturday.	For each incident where the reports are not available as defined in Section 3, a **$100 credit** shall be applied.

Customer shall have the right to request and receive the credit(s) set forth in the table above on its next invoice in the event of failures to comply with the performance standard set forth above. Notwithstanding the foregoing, the total credits that Customer may receive in any given month shall be capped at five percent (5%) of the previous month's invoice. In no event will any credits, including those exceeding such five percent (5%) cap, carry forward

to apply against future invoices. The credits set forth in this Service Level Addendum shall be the sole and exclusive remedy of Customer, and CS's entire liability for a failure to meet the performance standards and SLAs described herein.

Customer must promptly notify CS in the event any unscheduled downtime occurs. The obligations of CS set forth in this Service Level Addendum will be excused to the extent any failures to meet such obligations result in whole or in part from Customer's failure(s) to perform its obligations under the Agreement.

System Problem Resolution

Problems that impact availability of the System will be assigned a priority, resolution start time, and completion target interval, according to the following scale. CS will use commercially reasonable efforts to meet such standards.

Priority	Severity	Problem reporting and resolution coverage#	Resolution Start Time	Completion Target (Start-to-finish)
1	System unavailable or substantially inoperative	24 hours x 7 days/week	2 hours	2 hours
2	Significant impairment to System (e.g. reduced capacity, some users unable to login, etc.)	Regular business hours*	4 bus. hours	4 bus. hours
3	Minor impairment to System (e.g. completion problems to a particular destination country) exclusive of known limitations.	Regular business hours*	12 bus. hours	12 - 72 bus. hours

Notes:
Problems may be reported and will be addressed during the coverage periods shown.
* Regular business hours are 9 am - 5 pm Eastern time, Monday through Friday, Holidays excluded.

It is understood that general user support will be provided internally by the Customer. For the purpose of reporting system problems, the Customer will identify up to 4 contact people (names, contact data, and locations to be provided to CS) who will contact CS for all service problems. CS will provide contact lists (including 24-hour contact numbers) to the Customer for exclusive use by these Customer-designated trouble reporting contacts.

CS shall designate project manager(s) who shall serve as primary contact for resolving Customer problems during normal business hours. The primary point of contact for Customer will be _____.

Corrective Action

In the event that any SLA herein is not achieved, the specific performance objective will be noted and CS will develop a corrective action plan to achieve the standard. The action plan will then be monitored by CS to determine that the standard has been achieved.

ADAPTIVE SOLUTIONS SOFTWARE APPLICATION SERVICES ADDENDUM

This **ADAPTIVE SOLUTIONS SOFTWARE APPLICATION SERVICES ADDENDUM** (the "***Addendum***") is an addendum to, and is hereby incorporated into, that certain Master Services Agreement dated _____ ___, 20__ made by and between Contact Solutions, LLC (the "***Provider***") and _____ (together with its Affiliates, the "***Customer***"), including any amendments, exhibits, schedules, statements or work, work orders, change requests or other similar documents or agreements incorporated therein (collectively, the "***Agreement***").

1. DEFINITIONS.

Certain capitalized terms, not otherwise defined above, have the meanings set forth or cross-referenced in this Section 1 or the meanings set forth in the Agreement.

1.1 "***Addendum Term***" will have the meaning set forth in Section 6.1.

1.2 "***Affiliate***" means any entity controlling, controlled by or under common control with Customer.

1.3 "*Application*" means an interactive voice response software application provided by Provider to Customer pursuant to the Agreement.

1.4 "*Authorized Entity*" means the Customer's customer, whose Callers interact with the Software by way of their use of an Application. An Authorized Entity may be a commercial, private, non-governmental or a governmental organization. If the Authorized Entity is a governmental organization, the term shall only encompass the functional operating unit itself (i.e. agency, department, city, county or state) and by no means will include the entire government, whether local, state or federal.

1.5 "*Caller*" means an end user of an Application who is associated with a unique authentication or log-in ID whose interaction with the Application has been measured, or subject to measurement, by the Software.

1.6 "*Customer*" will have the meaning set forth in the preamble of this Addendum, above.

1.7 "*Services*" means the service described in Exhibit A.

1.8 "*Software*" means the software described in Exhibit A.

2. ACCESS AND USE.

2.1 Provision of Services. Subject to the terms and conditions contained in this Addendum, Provider agrees to provide the features and functions of the Services in connection with one or more Customer Applications (as identified in Exhibit A) during the Addendum Term solely for use by Customer, its Authorized Entity(ies) and its Callers solely in accordance with any documentation provided by Provider. Customer acknowledges and agrees that, as between Customer and Provider, Customer shall be responsible for all acts and omissions of Authorized Entities, and any act or omission by an Authorized Entity which, if undertaken by Customer, would constitute a breach of this Addendum, shall be deemed a breach of this Addendum by Customer.

2.2 Hosting Services. During the Addendum Term, Provider shall host the Software and make the features and functions of the Software available to Customer and its Authorized Entities in accordance with the terms of this Addendum. Customer understands that nothing in this Addendum may be interpreted to require delivery of a copy of the Software to Customer or installation of such a copy upon any computers or systems under Customer's control.

2.3 Usage Restrictions. Customer will not (i) decompile, disassemble, reverse engineer or otherwise attempt to obtain or perceive the source code from which any software component utilized to provide the Services is compiled or interpreted, and Customer acknowledges that nothing in this Addendum will be construed to grant Customer any right to obtain or use such source code; (ii) modify the Services or the Software, or create any derivative product from any of the foregoing, except with the prior written consent of Provider; or (iii) assign, sublicense, sell, resell, lease, rent or otherwise transfer or convey, or pledge as security or otherwise encumber, Customer's rights under this Section 2 (except for sales or resales by Customer to its Authorized Entities or other entities, in either case with the prior approval of Provider, which shall not be unreasonably withheld). Customer will ensure that its use of the Services complies with all applicable laws, statutes, regulations or rules.

2.4 Retained Rights; Ownership. Subject to the rights granted in this Addendum, Provider retains all intellectual property rights embodied in, or practiced by, the Services (or any component thereof or software or processes utilized to provide the same) and the Software, and Customer acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Addendum. Customer further acknowledges that Provider retains the right to use the foregoing for any purpose in Provider's sole discretion.

3. CUSTOMER OBLIGATIONS.

3.1 Authorized End User Access to Services. Subject to the terms and conditions herein, Customer may permit any Authorized Entity to use the features and functions of the Services in connection with one or more Customer Applications (as identified in Exhibit A). Customer will ensure that any such Authorized Entity will be bound by a contractual, enforceable agreement, which agreement, will, by its terms, (a) provide substantially the same or greater protections for Provider's Confidential Information, the Services and the Software and rights to data as are provided by the terms hereof and (b) be enforced by Customer.

3.2 Provision of Support to Customer. Support for the Services is available to Customer by telephone as specified in the Agreement in the section entitled "System Problem Resolution," with "System" therein referring to the Services for the purposes of this Addendum. Provider also reserves the right to make changes to the Services or the Software from time to time; provided that such changes will not materially reduce the functionality of the Services; such changes shall not preclude provision of the Services to Customer pursuant to this Addendum. Provider reserves the right, as required and without notice to Customer, to control, restrict, and/or disable the Services to prevent any negative impact to Customer or any other subscribers. Other than as required from Provider under this Section 3.2, Customer shall provide all maintenance and technical support services as may be required by its Authorized Entities with respect to use of the Services. In the event that any Customer Authorized Entity contacts Provider, Provider, in its discretion, may decline to provide such services and, at Customer's expense, redirect and/or refer such Authorized Entity to Customer at such point of contact as Customer may hereafter designate in writing to Provider.

3.3 Assistance to Provider. To the limited extent that may be reasonably necessary to enable Provider to perform its obligations hereunder, Customer will provide assistance to Provider, including, but not limited to, by means of access to, and use of, Customer facilities and Customer equipment, as well as by means of assistance from Customer personnel.

3.4 Customer Data. Customer acknowledges and understands that use of the Services will permit or require Customer to provide certain of Customer's data (including information provided by Authorized Entities and/or Callers) to Provider for purposes of processing or storage using the features and functions of the Services, including the information provided by Callers ("***Customer Data***"). All such Customer Data shall be considered proprietary to Customer, and Provider will not use such Customer Data except as necessary to perform under this Addendum. Customer Data that is personal health information (PHI) as defined in the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be de-identified and protected to the "safe harbor" standards of 45 C.F.R. Parts 160 and 164; Customer Data that is personally identifiable information (PII) shall be de-identified and protected to standards of the U.S. –European Union Safe Harbor Framework. Customer hereby grants to Provider a non-exclusive, non-transferable right and license to: (a) use the Customer Data

for the limited purposes of performing Provider's rights and obligations under this Addendum and (b) on a perpetual basis, (i) use, display, modify and create derivative works of the Customer Data solely to derive, create and compile aggregated statistics and/or data that is not personally attributable to or identified with Customer or any individual Caller ("***Aggregate Data***"); and (ii) copy, display, disclose, modify and distribute the Aggregate Data. Notwithstanding anything in this Addendum or the Agreement, Provider may, without liability or obligation, utilize its or its suppliers' database to confirm caller name, address and telephone number and may update and supplement such database with name, address and telephone number obtained as a result of providing the Services. Customer will have no express or implied right to license Provider's database or otherwise have any right to or in Provider's proprietary or licensed data. Customer acknowledges and agrees that, except as otherwise agreed between the Parties in an addendum to this Addendum or in a separate written agreement, Provider will have no obligation to archive or back-up Customer Data, nor will Provider have any liability for any loss or corruption of Customer Data (except as otherwise set forth herein), nor will Provider have any obligation under this Addendum to retain any Customer Data after the expiration or termination of the Addendum Term.

3.5 Transactional Data. Without limiting the provisions of Section 3.4, Provider may utilize data capture, syndication, and analysis tools, and other similar tools, to extract, compile, synthesize, and analyze Transactional Data. "***Transactional Data***" means any non-personally identifiable data or information resulting from a Caller's interaction with the Services (e.g., the number of Callers that press "1"). To the extent that any Transactional Data is collected by Provider, such Transactional Data will be solely owned by Provider and may be used by Provider for any lawful purpose, provided that the Transactional Data is used only in a de-identified and aggregated form and in a manner that does not permit the identification of Customer or any Caller. Provider agrees to comply with applicable privacy and other laws and regulations respecting the dissemination and use of such Transactional Data.

3.6 Professional Services. Customer may request that Provider provide certain professional services related to Customer's use of the Services, including, by way of example, customization of the Services. However, unless otherwise agreed between the parties in an addendum to this Addendum or in a separate written agreement, Provider shall have no obligation to provide or perform such services for or on behalf of Customer.

3.7 Proprietary Notices. Customer shall duplicate all proprietary notices and legends of Provider and its licensors upon any and all copies of any documentation made by Customer. Customer shall not remove, alter or obscure any such proprietary notice or legend. Customer shall create and maintain complete and accurate records of all copies of any documentation made by or on behalf of Customer, including the date such copies are made and where such copies are located. Customer shall promptly provide a copy of such records upon request by Provider.

4. FEES AND PAYMENTS.

4.1 Payment Obligation. In consideration for the rights granted to Customer and the performance of Provider's obligations under this Addendum, Customer shall pay to Provider, without offset or deduction, certain fees in such amounts as may be determined by reference to Exhibit A to this Addendum. Unless otherwise provided in such Exhibit A, all such fees shall be due and payable within thirty (30) calendar days after an invoice is issued by Provider with respect thereto.

4.2 Suspension of Service. In the event that Customer's account is more than thirty (30) days overdue, Provider shall have the right in its sole discretion, in addition to its remedies under this Addendum or the Agreement or pursuant to applicable law, to suspend Customer's use of the Services, without further notice to Customer, until Customer has paid the full balance owed, plus any interest due in accordance with the Agreement.

5. WARRANTIES AND LIMITATIONS.

5.1 Limited Provider Warranties. Provider warrants that the Services will conform in all material respects to the service standards set forth in Exhibit A when accessed and used in strict accordance with the terms and conditions described herein. Notwithstanding any other provision of this Addendum, Customer acknowledges and agrees that its sole and exclusive remedy, and Provider's sole and exclusive obligation, with respect to any breach of the foregoing warranty shall be termination for breach pursuant to Section 6.2 below.

5.2 Limitations of Warranty and Liability. Except as expressly set forth in Section 5.1 of this Addendum, Provider makes no representations or warranties under this Addendum, and Customer acknowledges that this Addendum is subject to all disclaimers and limitations or liability set forth in the Agreement.

6. ADDENDUM TERM AND TERMINATION.

6.1 Addendum Term. This Addendum shall become effective as of the date hereof; the initial one-year term shall begin upon the initial date of implementation of the Services; and the term shall continue in full force and effect in one-year periods for each Application to which the Services are applied unless terminated in accordance with the terms established in Exhibit A or in accordance with this Section. The period during which this Addendum remains in effect shall be the "***Addendum Term***". Unless otherwise agreed by the parties in Exhibit A of this addendum, upon expiration of the Addendum Term this agreement shall automatically renew for the same term, unless either party has given written notice of its intent not to renew this Agreement at least thirty (30) days prior to the end of the then-current term.

6.2 Termination for Breach. Either Party may, at its option, terminate this Addendum in the event of a material breach by the other Party. Such termination may be effected only through a written notice to the breaching Party, specifically identifying the breach or breaches on which such notice of termination is based. The breaching Party will have a right to cure such breach or breaches within thirty (30) days of receipt of such notice, and this Addendum shall terminate in the event that such cure is not made within such thirty (30)-day period. Without limiting the foregoing, Provider may immediately terminate this Addendum upon written notice in the event that Customer breaches Section 2.3 of this Addendum or becomes insolvent or enters bankruptcy prior to payment of all amounts due under Section 4 of this Addendum.

6.3 Effect of Termination. Upon any termination of this Addendum, Customer shall (i) immediately discontinue all use of the Services; (ii) return all documentation to Provider, if any; and (iii) promptly pay to Provider all amounts due and remaining payable under this Addendum.

6.4 Survival. The provisions of Sections 2.3, 2.4, 4, 6, 6.3, and 6.4 will survive the termination of this Addendum.

* * * * * * *

The parties agree to the above terms and have executed this Addendum as of the date(s) set forth below.

CUSTOMER: _____	**CONTACT SOLUTIONS, LLC**
By (Signature): _____	**By (Signature):** _____
Name (Printed): _____	**Name (Printed):** Bridget Lange
Title: _____	**Title:** VP, Finance & Administration
Date: _____	**Date:** _____

Exhibit A

DESCRIPTION OF ADAPTIVE PERSONALIZATION – ADAPTIVE RECALL SOFTWARE AND SERVICES; PRICING SCHEDULE

Adaptive Recall is a software solution that tracks user preferences over time based on the phone number, or ANI that they are calling from. Adaptive Recall tracks the ANI, authentication credentials, and menu selections to learn a caller's preferences. If a caller selects the same menu choices 'n' times in a row where n is configurable, then Adaptive Recall will use those learned preferences to personalize the caller experience in subsequent authenticated calls from that phone number.

The Adaptive Recall solution will provide for up to 3 application configurations as follows:

- Streamlined Authentication – Once a user has been personalized with Adaptive Recall, you may be able to reduce the amount of data required to authenticate a user.
- Skip a Menu – If a user has shown a preference for selecting a certain option on the menu, then Adaptive Recall will identify their preference and skip the menu altogether. One prime example of this option is to learn a caller's language preference and skip the Language Menu.
- Push Data – If a user has shown a preference for selecting a particular option in the call flow, then Adaptive Recall will identify this preference and push the data directly to the caller. A prime example of this option is to learn that a caller primarily selects to hear their balance so the balance information is pushed to the caller without them having to go through the menu options.

The "***Services***" are generally described below as the delivered capabilities, with the understanding that the provision of the Application(s) is not considered a part of the Services. The specific Services to be provided to any specific Authorized Entity shall be designated expressly in a task order or in a change request, as described below in the section entitled "Authorized Entities; Change Process" found below

[Insert Customer-specific description of delivery, implementation, services included in the pricing below, list of one or more applications to which AS will be applied.]

PRICING

Adaptive Personalization Application Modifications		
One Time Fees	**List Price**	**Includes**
Adaptive Recall	xxxx	Streamlined authentication, skip a menu (e.g. Language menu), and a push of one piece of data (e.g. Balance or last transactions)

Adaptive Personalization per Call Fees	
Adaptive Recall	**List Price**
Per Call	$ xxxx

AUTHORIZED ENTITIES; CHANGE PROCESS

Customer may establish Authorized Entities and the scope of Services to be provided thereto pursuant to this Addendum at any time pursuant to (a) a work order drafted by Provider on Provider's form of work order and executed by and between Customer and Provider or (b) a change request made to Provider and executed by Customer and Provider on Provider's form of change request. Such work orders or change requests shall include, at a minimum, the name of the proposed Authorized Entity(ies), the Applications to which the Services shall be applied, the scope of such Services to be applied, the pricing and payment terms, and the term of such Services, all subject to the terms and conditions described herein. Provider shall have no obligation to provide the Services to any party not made an Authorized Entity to this Addendum pursuant to this process.

Exhibit B

DESCRIPTION OF ADAPTIVE PERSONALIZATION – ADAPTIVE AUDIO SOFTWARE AND SERVICES; PRICING SCHEDULE

Adaptive Solutions is a patented set of software products (the "***Software***") which are separate and distinct from the Customer Application(s) and have been designed, developed, and will be delivered by Provider to the Customer pursuant to the terms and conditions of the Addendum and the Agreement.

Adaptive Audio adjusts Application call speed and content based on data from Adaptive Intelligence, as well as real-time, individual caller behavior. Adaptive Audio uses data from Adaptive Intelligence to improve customer experience in an Application by recognizing Caller behavior, then automatically and dynamically adjusting call speed in real time to best address the demonstrated behavioral needs of Callers of various levels of expertise with the Application (and similar applications generally). Adaptive Audio, when activated, will automatically speed up or slow down the pacing (words per minute) of the call, referred to as Adaptive Playback Control.

The "***Services***" are generally described below as the delivered capabilities, with the understanding that the provision of the Application(s) is not considered a part of the Services. The specific Services to be provided to any specific Authorized Entity shall be designated expressly in a task order or in a change request, as described below in the section entitled "Authorized Entities; Change Process" found below.

[Insert Customer-specific description of delivery, implementation, services included in the pricing below, list of one or more applications to which AS will be applied.]

PRICING

Adaptive Personalization Application Modifications		
One Time Fees	**List Price**	**Includes**
Adaptive Audio	xxxx	Adaptive playback control with 3 different voice speeds

Adaptive Personalization per Call Fees	
Adaptive Audio	**List Price**
Per Call	$ xxxx

AUTHORIZED ENTITIES; CHANGE PROCESS

Customer may establish Authorized Entities and the scope of Services to be provided thereto pursuant to this Addendum at any time pursuant to (a) a work order drafted by Provider on Provider's form of work order and executed by and between Customer and Provider or (b) a change request made to Provider and executed by Customer and Provider on Provider's form of change request. Such work orders or change requests shall include, at a minimum, the name of the proposed Authorized Entity(ies), the Applications to which the Services shall be applied, the scope of such Services to be applied, the pricing and payment terms, and the term of such Services, all subject to the terms and conditions described herein. Provider shall have no obligation to provide the Services to any party not made an Authorized Entity to this Addendum pursuant to this process.

ADAPTIVE SOLUTIONS SOFTWARE APPLICATION SERVICES ADDENDUM

This **ADAPTIVE SOLUTIONS SOFTWARE APPLICATION SERVICES ADDENDUM**, including any and all Addendum Exhibits (as defined below) attached hereto and incorporated herein (collectively, the "***Addendum***"), is an addendum to, and is hereby incorporated into, that certain Master Services Agreement, dated _____ ___, 20__, made by and between Contact Solutions, LLC (the "***Provider***") and _____ (together with its Affiliates, the "***Customer***"), including any amendments, exhibits, schedules, statements of work, work orders, change requests or other similar documents or agreements incorporated therein (collectively, the "***Agreement***").

1. DEFINITIONS.

Certain capitalized terms, not otherwise defined above, have the meanings set forth or cross-referenced in this Section 1 or the meanings set forth elsewhere in this Addendum or in the Agreement.

1.1 "*Addendum Exhibit*" means any exhibit to this Addendum that is signed by an authorized representative of Provider and Customer (individual Addendum Exhibits shall be denoted as follows: "Exhibit A," "Exhibit B," etc.).

1.3 "*Affiliate*" means any entity controlling, controlled by or under common control with Customer.

1.4 "*Application*" means an interactive voice response software application provided by Provider to Customer pursuant to the Agreement.

1.5 "*Authorized Entity*" means the Customer's customer, whose Callers interact with the Software by way of their use of an Application. An Authorized Entity may be a commercial, private, non-governmental or a governmental organization. If the Authorized Entity is a governmental organization, the term shall only encompass the functional operating unit itself (i.e., agency, department, city, county or state) and by no means will include the entire government, whether local, state or federal.

1.6 "*Caller*" means an end user who interacts with an Application and who is associated with a unique authentication or log-in ID, whose interaction with the Application has been measured, or is subject to measurement, by the Software.

1.7 "*Customer*" will have the meaning set forth in the preamble of this Addendum, above.

1.8 "*Services*" means the service(s) described in any Addendum Exhibit.

1.9 "*Software*" means the software application(s) described in any Addendum Exhibit.

2. ACCESS AND USE.

2.1 Provision of Services. Subject to the terms and conditions contained in this Addendum, Provider agrees to provide the features and functions of the Services in connection with one or more Customer Applications (as identified in an applicable Addendum Exhibit) during the Addendum Term, solely for use by Customer, its Authorized Entity(ies) and its Callers, solely in accordance with any documentation provided by Provider. Customer acknowledges and agrees that, as between Customer and Provider, Customer shall be responsible for all acts and omissions of Authorized Entities, and any act or omission by an Authorized Entity which, if undertaken by Customer, would constitute a breach of this Addendum, shall be deemed a breach of this Addendum by Customer.

2.2 Hosting Services. During the Addendum Term, Provider shall host the Software and make the features and functions of the Software available to Customer and its Authorized Entities in accordance with the terms of this Addendum. Customer understands that nothing in this Addendum may be interpreted to require delivery of a copy of the Software to Customer or installation of such a copy upon any computers or systems under Customer's control.

2.3 Usage Restrictions. Customer will not (i) decompile, disassemble, reverse engineer or otherwise attempt to obtain or perceive the source code from which any Software component utilized to provide the Services is compiled or interpreted, and Customer acknowledges that nothing in this Addendum will be construed to grant Customer any right to obtain or use such source code; (ii) modify the Services or the Software, or create any derivative product from any of the foregoing, except with the prior written consent of Provider; or (iii) assign, sublicense, sell, resell, lease, rent or otherwise transfer or convey, or pledge as security or otherwise encumber, Customer's rights under this Section 2 (except for sales or resales by Customer to its Authorized Entities or other entities, in either case with the prior written approval of Provider, which shall not be unreasonably withheld). Customer will ensure that its use of the Services complies with all applicable laws, statutes, regulations or rules.

2.4 Retained Rights; Ownership. Subject to the rights granted in this Addendum, Provider retains all intellectual property rights embodied in, or practiced by, the Software and/or Services (or any component thereof or software or processes utilized to provide the same), and Customer acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Addendum. Customer further acknowledges that Provider retains the right to use the foregoing for any purpose in Provider's sole discretion.

3. CUSTOMER OBLIGATIONS.

3.1 Authorized End User Access to Services. Subject to the terms and conditions herein, Customer may permit any Authorized Entity to use the features and functions of the Services in connection with one or more Customer Applications (as identified in an Addendum Exhibit). Customer will ensure that any such Authorized Entity will be bound by an enforceable agreement, which agreement (a) will, by its terms, provide substantially the same or greater protections for Provider's Confidential Information, the Services and the Software, and rights to data as are provided by the terms hereof and (b) will be enforced by Customer.

3.2 Provision of Support to Customer. Support for the Services is available to Customer by telephone as specified in the Agreement in the section entitled "System Problem Resolution," with "System" therein referring to the Services for the purposes of this Addendum. Provider also reserves the right to make changes to the Services or the Software from time to time; provided that such changes will not materially reduce the functionality of the Services; such changes shall not preclude provision of the Services to Customer pursuant to this Addendum. Provider reserves the right, as required and without notice to Customer, to control, restrict, and/or disable the Services to prevent any negative impact to Customer or any other subscribers. Other than as set forth in this Section 3.2, Customer shall provide all maintenance and technical support services as may be required by its Authorized Entities with respect to use of the Services. In the event that any Customer Authorized Entity contacts Provider, Provider, in its discretion, may decline to provide such maintenance and technical support services and, at Customer's expense, redirect and/or refer such Authorized Entity to such Customer point of contact as Customer may designate in writing to Provider.

3.3 Assistance to Provider. To the limited extent reasonably necessary to enable Provider to perform its obligations hereunder, Customer will provide assistance to Provider, including, but not limited to, by means of access to, and use of, Customer facilities and Customer equipment, as well as by means of assistance from Customer personnel.

3.4 Customer Data. Customer acknowledges and understands that use of the Services will permit or require Customer to provide to Provider certain of Customer's data (including information provided by Authorized Entities and/or Callers) for purposes of processing or storage using the features and functions of the Services, including the information provided by Callers ("***Customer Data***"). All such Customer Data shall be considered proprietary to Customer, and Provider will not use such Customer Data except as necessary to perform under this Addendum. Customer Data that is personal health information (PHI) as defined in the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be de-identified and protected to the "safe harbor" standards of 45 C.F.R. Parts 160 and 164; Customer Data that is personally identifiable information (PII) shall be de-identified and protected to standards of the U.S. – European Union Safe Harbor Framework. Customer hereby grants to Provider a non-exclusive, non-transferable right and license: (a) to use the Customer Data for the limited purposes of exercising Provider's rights and fulfilling Provider's obligations under this Addendum and (b) on a perpetual basis, (i) to use, display, modify and create derivative works of the Customer Data solely to derive, create and compile aggregated statistics and/or data that is not personally attributable to or identified with Customer or any individual Caller ("***Aggregate Data***"); and (ii) to copy, display, disclose, modify and distribute the Aggregate Data. Notwithstanding anything in this Addendum or the Agreement to the contrary, Provider may, without liability or obligation, utilize its or its suppliers' database to confirm Caller name, address and telephone number and may update and supplement such database with name, address and telephone number obtained as a result of providing the Services. Customer will have no express or implied right or license to Provider's database or otherwise have any right to or in Provider's proprietary or licensed data. Customer acknowledges and agrees that, except as otherwise agreed between the Parties in an addendum to this Addendum or in a separate written agreement, Provider will have no obligation to archive or back-up Customer Data, nor will Provider have any liability for any loss or corruption of Customer Data (except as otherwise set forth herein), nor will Provider have any obligation under this Addendum to retain any Customer Data after the expiration or termination of the Addendum Term.

3.5 Transactional Data. Without limiting the provisions of Section 3.4, Provider may utilize data capture, syndication, and analysis tools, and other similar tools, to extract, compile, synthesize, and analyze Transactional Data. "***Transactional Data***" means any non-PII or dataresulting from a Caller's interaction with the Services (e.g., the number of Callers that press "1"). To the extent that any Transactional Data is collected by Provider, such Transactional Data will be solely owned by Provider and may be used by Provider for any lawful purpose, provided that the Transactional Data is used only in a de-identified and aggregated form and in a manner that does not permit the identification of Customer or any Caller. Provider agrees to comply with applicable privacy and other laws and regulations respecting the dissemination and use of such Transactional Data.

3.6 Professional Services. Customer may request that Provider provide certain professional services related to Customer's use of the Services, including, by way of example, customization of the Services. However, unless otherwise agreed between the parties in an addendum to this Addendum or in a separate written agreement, Provider shall have no obligation to provide or perform such services for or on behalf of Customer.

3.7 Proprietary Notices. Customer shall duplicate all proprietary notices and legends of Provider and its licensors upon any and all copies of any documentation made by Customer. Customer shall not remove, alter or obscure any such proprietary notice or legend. Customer shall create and maintain complete and accurate records of all copies of any documentation made by or on behalf of Customer, including the date such copies are made and where such copies are located. Customer shall promptly provide a copy of such records upon request by Provider.

4. FEES AND PAYMENTS.

4.1 Payment Obligation. Customer shall pay to Provider, without offset or deduction, the fees listed in Exhibit A. Unless otherwise provided in an Addendum Exhibit, all fees shall be due within thirty (30) calendar days after an invoice is issued by Provider with respect thereto.

4.2 Suspension of Service. In the event that Customer's account is more than thirty (30) days overdue, Provider shall have the right in its sole discretion, in addition to its remedies under this Addendum or the Agreement or pursuant to applicable law, to suspend Customer's use of the Services, without further notice to Customer, until Customer has paid

the full balance owed, plus any interest due in accordance with the Agreement.

5. WARRANTIES AND LIMITATIONS.

5.1 Limited Provider Warranties. Provider warrants that the Services will conform in all material respects to the service standards set forth in the applicable Addendum Exhibit when accessed and used in strict accordance with the terms and conditions described herein. Notwithstanding any other provision of this Addendum, Customer acknowledges and agrees that its sole and exclusive remedy, and Provider's sole and exclusive obligation, with respect to any breach of the foregoing warranty shall be Customer's rights set forth in Section 6.2 below.

5.2 Limitations of Warranty and Liability. Except as expressly set forth in Section 5.1 of this Addendum, Provider makes no representations or warranties under this Addendum, and Customer acknowledges that this Addendum is subject to all disclaimers and limitations of liability set forth in the Agreement.

6. ADDENDUM TERM AND TERMINATION.

6.1 Addendum Term. This Addendum shall become effective as of the date hereof; an initial term of one (1) year shall begin upon the initial date of implementation of the Services; and the term shall continue in full force and effect in one-year periods for each Application to which the Services are applied, unless terminated in accordance with the terms established in an Addendum Exhibit or in accordance with this Section. The period during which this Addendum remains in effect shall be the "***Addendum Term***". Unless otherwise agreed by the parties in an Addendum Exhibit, upon expiration of the Addendum Term this Addendum shall automatically renew for the same term, unless either party has given written notice of its intent not to renew this Addendum at least thirty (30) days prior to the end of the then-current term.

6.2 Effect of Termination. Upon any termination of this Addendum, Customer shall (i) immediately discontinue all use of the Services; (ii) return all documentation to Provider, if any; and (iii) promptly pay to Provider all amounts due and remaining payable under this Addendum.

6.3 Survival. The provisions of Sections 2.3, 2.4, 4, 5, 6.3, and 6.4 will survive the termination of this Addendum.

* * * * * * *

The parties agree to the above terms and have executed this Addendum as of the date(s) set forth below.

[Customer Name]
By _____
Name _____
Title _____
Date _____

Contact Solutions

By _____
Name _____
Title _____
Date _____

Exhibit A

Adaptive Fraud Prevention

Adaptive Fraud Prevention contains three components: (1) Red Flag detection in the IVR, (2) ANI Verification using Pindrop Security's Phone Reputation Service (PRS), and (3) Automated Knowledge Based Authentication (KBA) using IDology. Red Flag detection and KBA are independent of each other and can be purchased separately.

Red Flag detection includes access to Pindrop Security's PRS and does not require a Customer to have a direct relationship with Pindrop Security.

Automated Knowledge-Based Authentication integrates the application with IDology's Expect ID IQ KBA solution. A Customer must have a direct contractual relationship with IDology in order to receive KBA. Any amounts charged to Customers by IDology are incremental to, and are not included within, the fees listed below.

The KBA solution requires the IVR to provide the following information to IDology: Social Security number, Name, Address, and Birth Date. These items must be available and accessible by the IVR to provide the appropriate data integration with IDology. The KBA development fee set forth below is for call flow modifications to enable the automation of KBA questions and to disposition calls based on the KBA results.

Adaptive Fraud One-Time Fees[1]

Item	List Price	Includes
Knowledge based authentication development	$5,000	– Knowledge based authentication (KBA) via IVR – Requires client services approval to ensure in scope
Red flag development	$5,000	– Integration with red flags and associated application updates – Integration with Pindrop – Requires client services approval to ensure in scope – Updates to the call flow for proactive call routing based on red flags

1: One-time fees only apply if real-time call flow modification is required. If only data/reports are required, one-time fees do not apply.

Adaptive Fraud Recurring Fees

Red flags with Pindrop is separate from KBA.

Tier[1]	List Price	Includes
Knowledge based authentication		
Per call fee	$0.50	– Integration with IDology – Charges are only for those calls that receive KBA Minimum of $1,000 monthly will be charged
Red flags monthly subscription		
Up to 1M calls	$10,000	– Reporting and data storage – Daily automated rules based data analysis – Pindrop for suspicious/flagged calls only – Quarterly review of rules and call flow with Customer
1M to 5M calls	$25,000	
More than 5M calls	$50,000	

1: Based on all calls, not just suspected fraudulent calls.