

STATE OF NEW JERSEY

PARTICIPATING ADDENDUM AND STANDARD TERMS AND CONDITIONS

Under

**NASPO ValuePoint Contract for Cloud Solutions
[State of Utah Master Contract Number AR2478]**

This Participating Addendum is made as of the last date of signature below (the "Effective Date"), by and between, CSRA State and Local Solutions, LLC, whose address is 3170 Fairview Park Drive, Falls Church, VA 22042 ("Contractor"), and the State of New Jersey, Department of the Treasury, Division of Purchase and Property ("Participating State" or "State") whose address is 33 West State Street, 8th Floor, P.O. Box 039, Trenton, New Jersey 08625, on behalf of the State of New Jersey and all "Authorized Purchasers" (as defined below). For clarification of references throughout this document, the term "State," in any form, refers to the State and any Authorized Purchaser, unless otherwise indicated. Capitalized terms used but not defined shall have the meaning ascribed to them in the Original Master Agreement (as defined below).

WHEREAS, pursuant to N.J.S.A. 52:34-6.2, the Director of the Division of Purchase and Property (the "Director"), within the Department of the Treasury (the "Division") "may enter into cooperative purchasing agreements with one or more states for the purchase of goods and services;" and

WHEREAS, the State of Utah ("Lead State") and Contractor have entered into Master Agreement #AR2478 (the "Master Agreement"), which may be found at the following URL: <http://www.naspovaluepoint.org/#/contract-details/71/overview/general>, awarded in accordance with the State of Utah Solicitation CH16012 for Cloud Solutions; and

WHEREAS, the State of New Jersey participated in the publicly advertised, competitive bidding process with fifteen other states and evaluated the proposals; and

WHEREAS, the Director has determined that entering into a Participating Addendum with Contractor under the Master Agreement to provide cloud solutions is the most cost effective method of procuring these Products and Services, and that it is in the best interest of the State to enter into a Participating Addendum with Contractor; and

WHEREAS, the parties seek to enter into this Participating Addendum to memorialize the terms of their contractual relationship;

NOW THEREFORE, for good and valuable consideration, receipt of which hereby acknowledged, the parties to this Participating Addendum hereby agree as follows:

1.0 Term and Extension Option; Order of Precedence; Entire Agreement

1. The term of this Participating Addendum shall be effective from the Effective Date and shall continue for a period ending on the Termination Date of the Master Agreement or when this Participating Addendum is terminated in accordance with the Master Agreement or this Participating Addendum, whichever shall occur first. Notwithstanding anything to the contrary contained in the Master Agreement, the State reserves the right, in its sole discretion, to extend this Participating Addendum upon an extension of the Master Agreement under the same terms and conditions as stated in this Participating Addendum. There shall be no automatic renewals of the Participating Addendum.
2. The entire agreement, and all rights and obligations between the parties, shall consist of the following documents (which shall be collectively referred to as the "Agreement"):

- a. This Participating Addendum and the State of New Jersey Compliance Terms and Conditions, attached to the State of Utah Bid Solicitation CH16012 ("Solicitation") within Attachment E and attached hereto as Exhibit A;
 - b. The original Master Agreement Attachment A package, together with its exhibits, as applicable ("Original Master Agreement"), attached hereto as Exhibit B;
 - c. The Master Agreement, incorporated herein as Exhibit C;
 - d. The Solicitation;
 - e. The Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
 - f. A Service Level Agreement and/or Statement of Work issued against the Participating Addendum.
3. These documents shall be read to be consistent and complimentary. In the event of any conflict between the terms of the documents comprising the Agreement, the conflict shall be resolved by giving priority to these documents in the order listed above.
4. The Agreement sets forth the entire agreement between the parties and supersedes all previous communications, representations or agreements, whether oral or written, with respect to the subject matter hereof. No Contractor terms and conditions shall apply to this Participating Addendum except those that are expressly accepted by the Lead State and must be in writing and attached to the Master Agreement as an Exhibit or Attachment as of the Effective Date of this Participating Addendum.
5. In the event the Lead State approves Contractor to offer new or additional Products and Services under the Master Agreement after the Effective Date of this Participating Addendum and such Products or Services incorporate any different, inconsistent, or additional terms into the Master Agreement, including, but not limited to any software license agreement or service level agreement, such terms are subject to this Agreement as set forth below.
6. References to external documentation; Software License Agreements and Service Level Agreements -
 - a. Any external information incorporated by reference within any of the documents comprising the Agreement, including, without limitation, software license agreements or service level agreements, are subject to the terms and conditions of this Participating Addendum. In the event of a conflict, the terms of this Participating Addendum shall prevail.
 - b. Any changes in the information incorporated by reference by any of the documents that comprise the Agreement, including, without limitation, software license agreements or service level agreements, are subject to the terms and conditions of this Participating Addendum. In the event of a conflict, the terms of this Participating Addendum shall prevail.
 - c. Any reference in Contractor's documents to website URLs that contain additional terms and conditions are subject to the terms and conditions of this Participating Addendum. In the event of a conflict, the terms of this Participating Addendum shall prevail.
7. Amendments – This Participating Addendum may not be amended except in a writing signed by both parties.

2.0 Scope of Participating Addendum

1. The scope of Products and Services that may be procured by Authorized Purchasers defined in Section 6.0(1) of this Participating Addendum (State Agencies) shall be those Products and

Services established in the Scope Addendum attached to this Participating Addendum as Attachment 1 as may be amended by the parties in writing from time to time. For all other Authorized Purchasers, the full suite of Product and Service offerings available under the Master Agreement may be procured under this Participating Addendum.

2. Contractor shall demonstrate to the State that each Product or Service included in an order is within the scope of the Master Agreement as approved by the Lead State.

3.0 Reporting Requirements

The Contractor shall deliver a copy of the detailed sales data reports described in Section 42 of the Original Master Agreement ("Reports") to the Procurement Specialist and State Contract Manager within ten (10) days of providing the Reports to the Lead State and NASPO ValuePoint Cooperative Development Team. The Reports may be limited to Sales made to Authorized Purchasers under this Participating Addendum.

4.0 Restrictions

1. Any restrictions or limitations regarding the State's use of this Agreement will be set forth in the State's Method of Operation, as may be amended from time to time and posted on the State's website.
2. Financing, leasing, and renting is not permitted under this Participating Addendum for State agencies. Authorized Purchasers, as defined in Section 6.0(2)-(5) may finance their purchase, if permitted under law. If financing is through a lease agreement, that agreement is separate from this Participating Addendum and is between the Contractor and the respective Authorized Purchaser only.

5.0 Termination of Contract

1. For Convenience-
 - A. Notwithstanding any provision or language in the Agreement to the contrary, the Director may terminate at any time, in whole or in part, this Participating Addendum or any contract entered into pursuant to this Participating Addendum, for the convenience of the State, upon no less than forty-five (45) days written notice to the Contractor.
 - B. Contractor shall not have the right to terminate this Participating Addendum for convenience.
2. For cause-
 - A. Where the Contractor fails to perform or comply with the Agreement or a portion thereof, and/or fails to comply with the complaints procedure in N.J.A.C. 17: 12-4.2 et seq., the Director may terminate this Participating Addendum, in whole or in part, upon thirty (30) days' notice to the Contractor with an opportunity to respond and cure within the thirty day period.
 - B. Where in the reasonable opinion of the Director, the Contractor continues to perform poorly under the Agreement as demonstrated by e.g., formal complaints, late delivery, poor performance of service, short-shipping, so that the Director is required to use the complaints procedure in N.J.A.C. 17:12-4.2 et seq., and there has been a failure on the part of the Contractor to make progress towards ameliorating the issue(s) or problem(s) set forth in the complaint the Director may terminate this Participating Addendum, in whole or in part, upon thirty (30) days' notice to the Contractor with an opportunity to respond prior to termination.

3. In cases of emergency the Director may shorten the time periods of notification and may dispense with an opportunity to respond.
4. In the event of termination under this section, the Contractor will be compensated for work performed or goods supplied in accordance with the Agreement, up to the date of termination. Such compensation may be subject to adjustments. In the event of a termination for convenience under Section 5.0(1), there shall be no refund of pre-paid fees. In the event of a termination for cause under Section 5.0(2), Contractor shall issue Authorized Purchaser(s) a pro-rata refund of unused pre-paid fees.
5. The Contractor shall not have the right to terminate this Participating Addendum. Any provisions in the Agreement regarding the Contractor's right to terminate or cancel this Participating Addendum are superseded by and replaced in their entirety by this Section 5.0 of this Participating Addendum. However, in the event that an Authorized Purchaser violates its obligations under the Agreement, Contractor may refuse to accept or process orders from such Authorized Purchaser immediately upon written notice to the State and such Authorized Purchaser, until such time as Authorized Purchaser submits a plan to correct such violations satisfactory to Contractor, which approval will not be unreasonably withheld. Notwithstanding anything to the contrary, Contractor shall continue to process orders submitted by other Authorized Purchasers. Section 7, Termination and Suspension of Service, in the applicable Exhibit to the Original Master Agreement shall apply in the event of a termination or cancellation pursuant to this section.
6. Any termination under this provision shall not affect the rights and obligations attending Orders outstanding at the time of termination, including but not limited to any right of any Authorized Purchaser 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 in an applicable Service Level of Agreement or Statement of Work, Contractor obligations under Section 7, Termination and Suspension of Service, in the applicable Exhibit to the Original Master Agreement, and any responsibilities arising out of a Security Incident or Data Breach.
7. The State may, for valid reason, issue a stop order directing the Contractor to suspend Products, work, and/or Services for a specific time. The Contractor shall be paid for Products ordered, Products delivered, and Services requested and performed until the effective date of the stop order. The Contractor shall resume Products, work, and/or Services upon the date specified in the stop order, or upon such other date as the State Contract Manager may thereafter direct in writing. The period of suspension shall be deemed added to the Contractor's approved schedule of performance. The Director may make an equitable adjustment, if any is required, to the Statement of Work price. The Contractor shall provide whatever information that Director may require related to the equitable adjustment. In the event Contractor disagrees with the final adjusted contract price, Section 12.0 (Miscellaneous – Alternative Dispute Resolution) shall apply. Section 7, Termination and Suspension of Service, in the applicable Exhibit to the Original Master Agreement shall apply in the event of a suspension made pursuant to this section.
8. Notwithstanding anything to the contrary in any of the documents comprising the Agreement, Orders shall not automatically renew. Following the expiration of an Order's term, Contractor shall treat such period as a suspension under Section 7, Termination and Suspension of Service, of the applicable Exhibit to the Original Master Agreement, unless the Authorized Purchaser notifies Contractor in writing of an intent not to renew in which case the remaining provisions of Section 7, Termination and Suspension of Service, shall apply.

6.0 Authorized Purchasers

"Authorized Purchasers" under this Participating Addendum shall mean the State and the following:

State of New Jersey Participating Addendum

1. State agencies.
2. Quasi-State Agencies - A "Quasi-State Agency" is any agency, commission, board, authority or other such governmental entity which is established and is allocated to a State department or any bi-state governmental entity of which the State of New Jersey is a member, as defined in N.J.S.A. 52:27B-56.1, provided that any sale to any such bi-state governmental entity is for use solely within the State of New Jersey.
3. Political Subdivisions, Volunteer Fire Departments And First Aid Squads, And Independent Institutions Of Higher Education - Counties, municipalities and school districts as defined in N.J.S.A. 52:25-16.1., volunteer fire departments, volunteer first aid squads and rescue squads as defined in N.J.S.A. 52:25-16.2, independent institutions of higher education as defined in N.J.S.A. 52:25-16.5, provided that each purchase by the independent institution of higher education shall have a minimum cost of \$500. The extension to counties, municipalities, school districts, volunteer fire departments, first aid squads and independent institutions of higher education must be under the same terms and conditions, including price, applicable to the State.
4. State Colleges –in accordance with N.J.S.A. 18A:64-60.
5. County Colleges - in accordance with N.J.S.A. 18A:64A- 25.9.

Authorized Purchasers as defined in Section 6.0(2)-(5) are responsible for the full cost of their purchases. The State and Authorized Purchasers as defined in Section 6.0(1) are responsible for the full cost of their purchases.

7.0 Modified Original Master Agreement Terms

1. **Section 8 Confidentiality, Non-Disclosure, and Injunctive Relief**, in the Original Master Agreement is amended to add the following:
 - e. The State's obligation to maintain the confidentiality of Contractor Confidential Information (as defined below) provided to the State under the Agreement is conditioned upon and subject to the State's obligations under the New Jersey Public Records Act, N.J.S.A. 47:1A-1 et seq., ("OPRA"), the New Jersey common law right to know, and any other lawful document request or subpoena.
 - f. Contractor's confidential information, to the extent not expressly prohibited by law, shall consist of all information clearly identified as confidential at the time of disclosure ("Contractor Confidential Information"). Notwithstanding the previous sentence, the Contractor acknowledges the terms and pricing of the contract are subject to disclosure under OPRA, the New Jersey common law right to know, and any other lawful document request or subpoena.
 - g. In the event that the State receives a request for Contractor Confidential Information related to the Agreement pursuant to a court order, subpoena, lawful document request or other operation of law, the State agrees, if permitted by law, to provide Contractor with as much notice, in writing, as is reasonably practicable and the State's intended response to such request. Contractor shall take any action it deems appropriate to protect its documents and/or information.
 - h. In addition, in the event Contractor receives a request for Confidential Information (as defined in the Original Master Agreement and amended by this Participating Agreement) pursuant to a court order, subpoena, or other operation of law, Contractor shall, if permitted by law, provide the State with as much notice, in writing, as is reasonably practicable and Contractor's intended response to such request. The State shall take any action it deems appropriate to protect its documents and/or information. Notice to the

State shall not relieve the Contractor of its obligation to take action to protect such information if the Contractor is aware of a legal reason to do so.

- i. Notwithstanding the requirements of nondisclosure described in this Section either party may release the other party's Confidential Information (i) if directed to do so by a court or arbitrator of competent jurisdiction, (ii) pursuant to a lawfully issued subpoena or other lawful document request, (a) in the case of the State, if the State determines the documents or information are subject to disclosure and Contractor does not exercise its rights as described in subsection (g) above, or if Contractor is unsuccessful in defending its rights as described in subsection (g), or (b) in the case of Contractor, if Contractor determines the documents or information are subject to disclosure and the State does not exercise its rights as described in subsection (h) above, or if the State is unsuccessful in defending its rights as described in subsection (h).
 - j. Except as permitted above and for confidentiality obligations related to information about a party's intellectual property, which shall never expire, neither party will use or disclose the other's Confidential Information for seven (7) years after the termination of the Agreement or such longer time period as required by applicable law.
2. **Section 13 Indemnification**, in the Original Master Agreement is amended to delete paragraph (a) and replace with the following:
 - 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 the negligent or willful 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.
3. **Section 13 Indemnification**, in the Original Master Agreement is amended to add the following:
 - c. Neither Contractor nor any attorney engaged by Contractor shall defend the claim in the name of the State of New Jersey or any Authorized Purchaser, nor purport to act as legal representative of the State of New Jersey or any Authorized Purchaser, without having provided notice to the Director of the Division of Law in the Department of Law and Public Safety and to the Director of DPP.
 - d. Notwithstanding anything to the contrary contained in the Agreement, the State shall not be responsible for the Contractor's attorney fees and/or expenses.
 - e. The Contractor's indemnification and liability is not limited by, but is in addition to the insurance obligations contained in the Agreement.
 - f. Notwithstanding anything to the contrary in the Agreement or any contract document, under no circumstances will the State indemnify, defend or hold harmless Contractor and any such provision in the Agreement or any contract document shall be of no force and effect. The State will not pay or reimburse for claims absent compliance with the terms of the New Jersey Tort Claims Act, N.J.S.A. 59:1-1 et seq. and the Contractual Liability Act, N.J.S.A. 59:13-1 et seq. and a determination by the State to pay the claim or a final order of a court of competent jurisdiction.
4. **Section 16 Insurance**, in the Original Master Agreement is amended as follows:
 - a. Subsection 16(b)(3) is amended to state the following:

- i. Worker's Compensation Insurance applicable to the laws of the State of New Jersey and Employers Liability Insurance with limits not less than:

\$1,000,000 BODILY INJURY, EACH OCCURRENCE

\$1,000,000 DISEASE EACH EMPLOYEE

\$1,000,000 DISEASE AGGREGATE LIMIT

- b. The following section is added as subparagraph (g):

- g. New Jersey Requirements:

- i. The Provider shall provide the State with current certificates of insurance for all coverages and renewals thereof. If the Provider receives a notice of cancellation, the Provider will promptly replace such coverage so that no lapse in insurance occurs.
 - ii. The Provider shall not begin to provide services or goods to the State until evidence of the required insurance is provided.
 - iii. The certificates of insurance shall indicate the contract number and title of the contract in the Description of Operations box and shall list the State of New Jersey, Department of the Treasury, Division of Purchase & Property, Contract Compliance & Audit Unit, PO Box 236, Trenton, New Jersey 08625 in the Certificate Holder box. The certificates shall be emailed to the State at ccau.certificate@treas.state.nj.us.

- 5. **Section 34 Assignment of Antitrust Rights**, in the Original Master Agreement is amended to add the following:

In connection with this assignment, the following are the express obligations of the Contractor:

- 1. It will take no action which will in any way diminish the value of the rights conveyed or assigned hereunder.
- 2. It will advise the Attorney General of New Jersey:
 - a. in advance of its intention to commence any action on its own behalf regarding any such claim or cause(s) of action;
 - b. immediately upon becoming aware of the fact that an action has been commenced on its behalf by some other person(s) of the pendency of such action.
- 3. It shall notify the defendants in any antitrust suit of the fact of the within assignment at the earliest practicable opportunity after the Contractor has initiated an action on its own behalf or becomes aware that such an action has been filed on its behalf by another person. A copy of such notice will be sent to the Attorney General of New Jersey.

Furthermore, it is understood and agreed that in the event any payment under any such claim or cause of action is made to the Contractor, it shall promptly pay over to the State of New Jersey the allotted share thereof, if any, assigned to the State hereunder.

8.0 Contractor Business Models; Roles and Responsibilities

- 1. Contractor may use one of three models, or a combination thereof, to provide Products and Services to Authorized Purchasers under this Agreement: (A) direct provision of Contractor's Products and Services, with or without Subcontractors (as that term is defined below), (B) offering of Fulfillment Partner Products and Services or (C) pass through of cloud service provider solutions.

- a. Where Contractor provides Contractor's Products and Services directly to Authorized Purchasers, Contractor may, with the prior written consent of the Director, utilize Subcontractors. As used in this Participating Addendum, Subcontractor shall mean an entity having an arrangement with Contractor, whereby Contractor uses the Products and/or Services of that entity to fulfill some of its obligations under this Agreement. Authorized Purchasers do not pay Subcontractors directly. Where Contractor utilizes a Subcontractor, Contractor shall provide to the State items 1 and 9, as enumerated in Section 14.0, The State of New Jersey Mandatory Certification Requirements, of this Participating Addendum ("Subcontractor Certifications") for each proposed Subcontractor along with Contractor's written request for approval thereof.
 - i. Where a Subcontractor is approved, Contractor may not substitute another Subcontractor without the prior written consent of the Director and until Contractor provides to the State Subcontractor Certifications for the new proposed Subcontractor along with Contractor's written request for approval thereof.
 - ii. If at the time of the execution of the Agreement, Contractor is generally utilizing a subcontractor to provide technical support and/or other non-contract related Services to its customers, such subcontractor need not be disclosed, and Contractor may substitute a different subcontractor without the Director's prior approval.
- b. In the event Contractor offers Fulfillment Partner Products and Services to Authorized Purchasers, each Fulfillment Partner must be approved by the State. Such approved Fulfillment Partner may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Products and Services under the Agreement and directly invoicing and receiving payment from Authorized Purchasers. A Fulfillment Partner has no authority to amend this Agreement or to bind Contractor, State, or Authorized Purchasers to any additional terms and conditions.
 - i. Contractor may add Fulfillment Partners to its Participating Addendum at any time during the contract term, upon the written consent of the Director. To add a Fulfillment Partner, Contractor shall submit to the State a written request with:
 - 1. Evidence that all Products and Services were approved by the Lead State under the Master Agreement; and
 - 2. Items 1 through 9, as enumerated in Section 14.0, The State of New Jersey Mandatory Certification Requirements, of this Participating Addendum for each Fulfillment Partner.
 - ii. In the event Contractor submits a written request to delete a Fulfillment Partner's Products and Services from the scope of Contractor's Participating Addendum, Contractor shall provide State and Authorized Purchaser(s) at least thirty (30) days' advance written notice of the request and shall, upon State or Authorized Purchaser request, provide State and Authorized Purchaser(s) assistance and advice regarding the exit and/or transition strategy for all digital content and Data (as that term is defined in the Original Master Agreement) affected by the requested deletion at no cost to the State or Authorized Purchaser. If the State approves the request to delete a Fulfillment Partner:
 - 1. The deletion shall not terminate the Participating Addendum or other Products and Services unaffected by the deletion, however, such Fulfillment Partner deletion shall be deemed a termination for cause for purposes of digital content and Data retention and destruction discussed in Section 7, Termination and Suspension of Service, in the applicable Exhibit to the Original Master Agreement; and
 - 2. In the event of any pre-paid fees for Products or Services to Contractor or Fulfillment Partner affected by the deletion, such Fulfillment Partner

deletion shall be deemed a termination for cause as to those pre-paid fees for purposes of Section 5.0(4) of this Participating Addendum.

- c. With the prior written consent of the Director, Contractor may pass through or resell third party cloud service provider Products and Services to Authorized Purchasers. Where Contractor is passing through third party cloud service provider Products and Services, the cloud service provider shall only provide web-based computing capabilities and related remote technical support. Authorized Purchasers shall not pay cloud service providers directly and cloud service providers shall not be deemed Subcontractors.
 - i. Where a third party cloud service provider is approved, Contractor may not substitute another cloud service provider without the prior written consent of the Director.
 - ii. In the event Contractor submits a written request to remove a cloud service provider's Products and Services from the scope of Contractor's Participating Addendum, Contractor shall provide State and Authorized Purchaser(s) at least thirty (30) days' advance written notice of the request and shall, upon State or Authorized Purchaser request, provide State and Authorized Purchaser(s) assistance and advice regarding the exit and/or transition strategy for all digital content and Data (as that term is defined in the Original Master Agreement) affected by the requested deletion at no cost to the State or Authorized Purchaser. If the State approves the request to delete a cloud service provider:
 1. The deletion shall not terminate the Participating Addendum or other Products and Services unaffected by the deletion, however, such cloud service provider deletion shall be deemed a termination for cause for purposes of digital content and Data retention and destruction discussed in Section 7, Termination and Suspension of Service, in the applicable Exhibit to the Original Master Agreement; and
 2. In the event of any pre-paid fees for Products or Services to Contractor or Fulfillment Partner affected by the deletion, such cloud service provider Partner deletion shall be deemed a termination for cause as to those pre-paid fees for purposes of Section 5.0(4) of this Participating Addendum.
2. Regardless of the model used and whether prior approval is required or given, Contractor shall remain primarily responsible to the State and Authorized Purchasers for all Products and Services provided to the State under the Agreement including, but not limited to: (I) performance; (II) compliance with all of the terms and conditions of the Agreement and (III) compliance with the requirements of all applicable laws. Furthermore, Contractor's use of one or more Subcontractors, Fulfillment Partners, or cloud service providers does not create privity of contract between any of the Subcontractors, Fulfillment Partners, or cloud service providers and the State.
3. This Participating Addendum may not be subcontracted or assigned by the Contractor, in whole or in part, without the prior written consent of the Director, which shall not be unreasonably withheld.
4. For the avoidance of doubt, the Contractor shall be responsible for obtaining all required forms outlined in Section 14.0, The State of New Jersey Mandatory Certification Requirements, of this Participating Addendum from each Subcontractor or Fulfillment Partner and submit the required forms to the State along with Contractor's written request for approval thereof. The State will not accept forms directly from a Subcontractor or Fulfillment Partner.

9.0 Ordering and Compensation

1. Pricing shall be in accordance with the terms set forth in the Master Agreement, as amended by this Participating Addendum.

2. The State of New Jersey Contract number and the Master Agreement number ("_____, AR2478") MUST be shown on all Service Level Agreements, Statement of Work documents, and Purchase Orders issued against this Participating Addendum.
3. All orders and payments will be issued to either the Contractor or the Fulfillment Partner and shall be in accordance with the terms set forth in the Agreement, as amended by this Section 9.0 of this Participating Addendum.
4. As stated in Section 5.0 Termination of Contract, Orders shall not automatically renew.
5. The State of New Jersey's obligation to make payment under the Agreement is contingent upon the availability of appropriated funds and receipt of revenues from which payment for contract purposes can be made. No legal liability on the part of the State of New Jersey for payment of any money shall arise unless and until funds are appropriated each fiscal year to the using agency which is an Authorized Purchaser by the New Jersey State Legislature and made available through receipt of revenues. Notwithstanding the foregoing, the parties agree that performance under this contract is contingent upon the appropriation of funds.
6. Contractors or Fulfillment Partners may be paid by the State through the Procurement card (p-card) at the time the original order is placed. P-card transactions do not require the submission of either a contractor invoice or a State payment voucher. Purchasing transactions utilizing the p-card will usually result in payment to the Contractor or the Fulfillment Partners in three (3) days. The Contractor and the Fulfillment Partner should take note that there will be a transaction processing fee for each p-card transaction. To participate, the Contractor or Fulfillment Partner must be capable of accepting the applicable credit card.
7. Payments shall be made to the Contractor or Fulfillment Partners pursuant to the provisions of the New Jersey Prompt Payment Act, N.J.S.A. 52:32-32 et seq. The Act requires state agencies to pay for goods and services within sixty (60) days of the state agency's receipt of a properly executed State Payment Voucher. Interest will be paid on delinquent accounts at a rate established by the New Jersey State Treasurer (the "State Treasurer"). Interest will not be paid until it exceeds \$5.00 per properly executed invoice.
8. Cash discounts and other payment terms included as part of the Agreement are not affected by the Prompt Payment Act.
9. Contractor and Fulfillment Partners are encouraged to offer cash discounts based on expedited payment by the State. The State will make efforts to take advantage of discounts, but discounts will not be considered in determining the lowest quote.

Discount periods shall be calculated starting from the next business day after the recipient has accepted the goods or services received a properly signed and executed State Payment Voucher form and, when required, a properly executed performance security, whichever is latest.
10. The date on the check issued by the State in payment of that Voucher shall be deemed the date of the State's response to that Voucher.

10.0 Additions to the State of New Jersey Compliance Terms and Conditions

1. Compliance With State Laws-

It is agreed and understood that any contracts and/or orders placed under this Participating Addendum and any claims and any and all litigation arising there from or related thereto shall be governed and construed and the rights and obligations of the parties hereto and of the Authorized Purchasers shall be

determined in accordance with the laws of the State of New Jersey, including without limitation, by the New Jersey Tort Claims Act, N.J.S.A. 59:1-1, et seq., the New Jersey Contractual Liability Act, N.J.S.A. 59:13-1, et seq., and governed by the applicable laws, regulations and rules of evidence of the State of New Jersey without reference to conflict of laws principles, and any and all litigation arising therefrom or related thereto shall be filed in the appropriate Division of the New Jersey Superior Court.

2. Open Public Records Act-

All documents and information submitted by Contractor to the State under this Participating Addendum are considered public information, notwithstanding any disclaimers to the contrary submitted by a Contractor, except as may be exempted from public disclosure by the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 et seq., and the common law.

3. Maintenance of Records-

The Contractor shall maintain records for products and/or services directly related to sales orders and corresponding invoices, including product specifications at time of shipping, issued in accordance with this Participating Addendum for a period of five (5) years from the date of final payment. Such records shall be made available to the State, including the State of New Jersey, Office of the State Comptroller, for audit and review.

4. Organ and Tissue Donation –

As required by N.J.S.A. 52:32-33.1, the State encourages Contractors to disseminate information relative to organ donation and to notify its employees, through information and materials or through an organ and tissue awareness program, of organ donation options. The information provided to employees should be prepared in collaboration with the organ procurement organizations designated pursuant to 42 U.S.C. §1320b-8 to serve in this State.

5. Tax Exemption-

The State of New Jersey is exempt from State sales or use taxes and Federal excise taxes. Therefore, price quotations must not include such taxes. The State's Federal Excise Tax Exemption number is 22-75-0050K.

11.0 Liabilities

1. Unless otherwise agreed in writing and signed by the Director, the following limitation of liability shall apply:
 - a. Contractor's liability arising out of or in connection with each Order(s) is limited to two times (2x) the amount paid by the State under the applicable Order(s) over the prior twelve months. Notwithstanding the preceding sentence, in no event shall the limit of liability be less than \$250,000.
 - b. In no event shall Contractor be liable for any punitive, special, indirect, or consequential damages arising out of this Participating Addendum.
 - c. This limitation of liability shall not apply to:
 - i. Contractor's obligation to indemnify, defend, and save harmless the State and its employees as described in Section 13, Indemnification, of the Original Master Agreement as amended by this Participating Addendum,
 - ii. Claims arising from Section 8, Confidentiality, Non-Disclosure, and Injunctive Relief, of the Original Master Agreement as amended by this Participating Addendum, or
 - iii. Claims arising from Section 30, Data Privacy, of the Original Master Agreement.

- d. Notwithstanding the foregoing exclusions, where 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 State, 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) completing all corrective actions as reasonably determined by Contractor based on root cause of the Data Breach.
2. Where Contractor, Authorized Purchaser, and the Director agree in writing to a different limitation of liability than that established in this Section 11.0 ("Negotiated LOL"), the Negotiated LOL shall only apply to the specific Order for that Authorized Purchaser. The Negotiated LOL shall not be deemed an amendment to this Participating Addendum. For the avoidance of doubt, all other terms of the Order shall be subject to the order of precedence established in Section 1.0 of this Participating Addendum.

12.0 Miscellaneous

1. Mergers, Acquisitions and Dissolutions-

Merger or Acquisition:

If, during the term of this Participating Addendum, the Contractor shall merge with or be acquired by another firm, the Contractor shall give notice to the Director as soon as practicable and in no event longer than thirty (30) days after said merger or acquisition. Any such merger or acquisition will require the assignment of the Agreement, as amended by this Participating Addendum, pursuant to the provisions related thereto set forth therein. The Contractor shall provide such documents as may be requested by the Director, which may include but need not be limited to the following: corporate resolutions prepared by the Contractor and new entity ratifying acceptance of the original contract, terms, conditions and prices; updated information including ownership disclosure and Federal Employer Identification Number. The documents shall be submitted within thirty (30) days of the request. Failure to do so may result in termination of this Participating Addendum for cause.

Dissolution:

If, during the term of this Participating Addendum, the Contractor's partnership, joint venture or corporation shall dissolve, the Director must be so notified. All responsible parties of the dissolved business entity must submit to the Director, in writing, the names of the parties proposed to perform under this Participating Addendum and the names of the parties to whom payment should be made. No payment will be made until all parties to the dissolved business entity submit the required documents to the Director.

2. Announcements and/or Advertisements-

All publicity and/or public announcements pertaining to this Participating Addendum shall be approved in writing by the State prior to release.

Contractor must obtain prior written (email) approval, no less than seven (7) business days before release for any and all advertisements pertaining to this Participating Addendum during its effective term. Any and all Fulfillment Partners may not directly send advertisements to any and all Authorized Purchasers without explicit written approval from the Contractor.

3. Contractor and/or Fulfillment Partner Audit-

The State and Authorized Purchasers reserve the right to audit the Contractor and/or Fulfillment Partner's compliance with the Agreement. Such audit shall be in accordance with Section 26, Records Administration and Audit, in the Original Master Agreement. The State or Authorized Purchaser shall provide Contractor and/or Fulfillment Partner thirty (30) days' written notice of intent to audit and such audit such be conducted during normal business hours.

4. Request for Additional Information-

The Director reserves the right to request relevant information from the Contractor, including factors necessary to evaluate the Contractor's financial capabilities to perform the Agreement.

5. Audit of Authorized Purchaser use of Intellectual Property -

1. Notwithstanding anything to the contrary in the Agreement , in the event that the Contractor seeks to exercise a right in the Agreement to audit the State's use of Contractor's intellectual property, the Contractor shall deliver simultaneous written notice, no less than thirty (30) days in advance of the audit start date (unless the Contractor's notice provides a longer notice period), to:
 - a. the Director of the New Jersey Department of Treasury, Division of Purchase and Property:
Procurement Bureau, Technology Unit
P.O. Box 230
Trenton, NJ 08625-0230
 - b. the Chief Data Officer of the New Jersey Office of Information Technology:
Office of the Chief Technology Officer
300 Riverview Plaza
Trenton, NJ 08625
 - c. and the State Contract Manager for this contract.
2. The notice shall reference the specific audit provision(s) in the Agreement being exercised and include copies of same, specify the means by which the Contractor will conduct the audit, and shall require the audit to be conducted in accordance with generally accepted standards in the field of such audits.
3. To the extent the agreement permits Contractor to conduct periodic audits of the State's usage of the Products and/or Services provided thereunder, such provision is amended to include the following dispute resolution process:

If the State, in good faith, provides Contractor with written notice of an alleged error in the amount of underpaid fees due Contractor as a result of an audit (the "dispute"), then the parties will endeavor to resolve the dispute in accordance with this paragraph. Each party will appoint a Vice President, Assistant Director, or the equivalent (hereinafter referred to as "Representative") to discuss the dispute and no formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief or those required to avoid non-compliance with the New Jersey Contractual Liability Act, N.J.S.A. 59:13-1 et seq., may begin until either such Representative concludes, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely. In addition, the parties shall refrain from exercising any termination right related to the dispute being considered under this paragraph and shall continue to perform their respective obligations under the license agreement, while they endeavor to resolve the dispute under this paragraph.
4. Notwithstanding anything to the contrary in the Agreement, the State will not pay or reimburse Contractor for costs or expenses associated with the performance of an audit.

5. In the event that the Agreement does not permit audits of the State's usage of the Contractor's Intellectual Property this provision shall not be interpreted to provide such an audit right.

6. Dispute Resolution –

The State and Contractor will attempt to resolve any dispute through face-to-face negotiation with persons fully authorized to resolve the dispute or through non-binding mediation utilizing a mediator agreed to by the parties, rather than through litigation. No formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief or those required to avoid non-compliance with the New Jersey Contractual Liability Act, N.J.S.A. 59:13-1 et seq., may begin until either such persons conclude, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely.

7. Arbitration or Mediation –

Any provision regarding arbitration or binding mediation within the Agreement is deleted in its entirety.

13.0 Waiver

No term or provision of this Participating Addendum shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by an individual authorized to so waive or consent. Any consent by either party to, or waiver of, a breach by the other whether expressed or implied, shall not constitute a consent to, waiver of, or excuse for, any other breach or any subsequent breach, except as may be expressly provided in the waiver or consent.

14.0 The State of New Jersey Mandatory Certification Requirements

The following are New Jersey procurement requirements that Contractor agrees to fulfill prior to the Effective Date. Some Authorized Purchasers may have additional requirements when placing an order and Contractor shall comply with same as necessary.

1. New Jersey Business Registration (N.J.S.A. 52:32-44);
2. Ownership Disclosure (N.J.S.A. 52:25-24.2);
3. Disclosure of Investment Activities in Iran (N.J.S.A. 52:32-55 et seq.)
4. Executed MacBride Principles (N.J.S.A. 52:34-12.2);
5. Completed Contractor Certification and Disclosure of Political Contributions (N.J.S.A. 19:44A-20:13 et. seq.);
6. Disclosure of Investigations and Actions Involving Bidder
7. Vendor Certification (P.L. 2005, c.271);
8. Proof of insurance as specified herein;
9. Proof of compliance with New Jersey Affirmative Action requirements (N.J.A.C. 17:27-1.1 et. seq.):
 - a. New Jersey Form AA-302 Affirmative Action Employee Information Report; or
 - b. New Jersey Affirmative Action Certificate; or
 - c. Federal Affirmative Action Approval Letter.

15.0 Primary Contacts

The Division of Purchase and Property contact for this Participating Addendum is as follows:

Name:	Joshua Descoteaux
Title:	Procurement Specialist
Participating Entity Name:	Division of Purchase and Property, Department of the Treasury

Address: State of New Jersey
33 West State Street, 8th Floor
PO Box 230
Trenton, New Jersey 08625-0230
Telephone: (609) 292-0365
Fax: (609) 292-5170
E-mail: Joshua.Descoteau@treas.nj.gov

The State Contract Manager for this Participating Addendum is as follows:

Name: Lynne Gash
Title: State Contract Manager
Participating Entity Name: Office of Information Technology,
State of New Jersey
Address: 300 Riverview Plaza
Trenton, New Jersey 08625
Telephone: (609) 777-4121
E-mail: Lynne.Gash@tech.nj.gov

The primary Contractor contact for this Participating Addendum is as follows:

Name: Tracy Archer
Title: Sr. Contracts Administrator
Contractor: CSRA State and Local Solutions LLC
Address: 3170 Fairview Park Dr.
Falls Church, VA 22042
Telephone: 202-360-2055
Fax:
E-mail: tracy.archer@csra.com

The parties hereto agree that this Participating Addendum may be executed in counterpart, each original signed page to become part of the original document.

[Remainder of page intentionally blank. Signature page to follow.]

IN WITNESS WHEREOF, authorized representatives of Contractor and the State have executed this Participating Addendum to be effective on the Effective Date.

State of New Jersey, Department of the Treasury, Division of Purchase and Property By: _____ Name: _____ Title: Director Date: _____	CSRA State and Local Solutions LLC By: <u>Tracy Archer</u> Name: <u>Tracy Archer</u> Title: <u>Sr. Contracts Administrator</u> Date: <u>08/30/2017</u>
Approved as to Form: Christopher S. Porrino Attorney General of the State of New Jersey By: _____ Name: _____ Title: Deputy Attorney General Date: _____	=

IN WITNESS WHEREOF, authorized representatives of Contractor and the State have executed this Participating Addendum to be effective on the Effective Date.

State of New Jersey, Department of the Treasury, Division of Purchase and Property By: <u></u> Name: <u>MAURICE A. GRIFFIN</u> Title: Director Date: <u>10/2/2017</u>	CSRA State and Local Solutions LLC By: <u></u> Name: <u>Tracy Archer</u> Title: <u>Sr. Contracts Administrator</u> Date: <u>08/30/2017</u>
Approved as to Form: Christopher S. Porrino Attorney General of the State of New Jersey By: <u></u> Name: <u>Christopher S. Porrino</u> Title: Deputy Attorney General Date: <u>9/6/2017</u>	=

Contract # AR2478**STATE OF UTAH COOPERATIVE CONTRACT**

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

CSRA State and Local Solutions LLC
Name
3170 Fairview Park Drive
Address
Falls Church VA 22042
City State Zip

LEGAL STATUS OF CONTRACTOR

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

Contact Person Mackenzie Sestak, Contracts Advisor Phone #703.641.3517 Email Mackenzie.Sestak@csra.com
Vendor # 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: 09/30/2016 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 the 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: N/A

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:
- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
 - 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

STATE

Contractor's signature

Date

Director, Division of Purchasing

Date

D. Jerome Scherzinger, II; Manager, Contracts
Type or Print Name and Title

Christopher Hughes

Division of Purchasing Contact Person

801-538-3254

Telephone Number

Fax Number

christopherhughes@utah.gov

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Term of the Master Agreement: 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 if defaults cannot be reasonably cured as allowed per Default and Remedies terms.

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 of Contractor's employees 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 either party to this Master Agreement or to a Participating State or Participating Entity, or the appointment of a receiver or similar officer for any such party or any of any such party's 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, the party claiming default shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which the non-defaulting party 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 defaulting party's liability for damages.

c. If a defaulting party is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, the defaulting party shall be in breach of its obligations under this Master Agreement and non-defaulting party 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) In the event of default by the Contractor, and to the extent permitted by the law of the Participating State or Participating Entity, the Lead State shall have the right to 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.

e. Notwithstanding the foregoing, damages attributable to Security incidents shall be subject to the Section of the Master Agreement titled "Limitation of Liability".

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar

days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

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

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

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

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

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

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

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

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

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

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

16. Insurance

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

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

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

(2) CLOUD MINIMUM INSURANCE COVERAGE:

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

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

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

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

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

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

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

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

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

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

19. Ordering

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

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

may select the quote that it considers most advantageous, cost and other factors considered.

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

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

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

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

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

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

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

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

20. Participants and Scope

- a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.
- b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.
- c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office³.
- d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. 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.

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.

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.

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 in accordance with FBI CJIS Policy CJISD-ITS-DOC-08140-5.5 06/01/2016 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 (excluding their commercial suppliers of solutions) 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 (excluding their commercial suppliers of solutions) 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 (excluding their commercial suppliers of solutions) to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor (excluding their commercial suppliers of solutions) 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 (excluding their commercial suppliers of solutions) 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 (excluding their commercial suppliers of solutions) shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

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

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

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

b. Contractor will perform materially as described in this Master Agreement, SLA,

Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

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

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

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

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

32. Transition Assistance:

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

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

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

33. Waiver of Breach:

Failure of a party 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 a party must be in writing. Waiver by a party of any default, right or remedy under this Master Agreement or Participating Addendum, or by Participating 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: If Contractor, at its option, re-performs the Services or replaces the Product that is the subject of, or gave rise to, the claim, Contractor's total liability will be limited to such re-performance. If (i) the claim or matter cannot be remedied by such re-performance; (ii) re-performance is not an applicable remedy; or (iii) re-performance is not provided, then Contractor's total aggregate liability for any and all claims under this Master Agreement will be limited to and shall not exceed: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services giving rise to the party's claim (said amount not to exceed a total of twelve months (12) months charges under the applicable purchase order) including indirect damages or (ii) five million dollars (\$5,000,000.00), whichever is greater to the Purchasing Entity.

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.
. (Personal data does not include the limited set of data in the Directory which is used to manage user accounts and contains the names and email address of licensed users.)
- 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. (Non-public data does not include the limited set of data in the Directory which is used to manage user accounts and contains the names and email address of licensed users.)
- 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 (or in accordance with a commercial service providers SLA in the licensing agreements) 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 (or in accordance with a commercial service providers SLA in the licensing agreement) 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 in accordance with a commercial service providers SLA in the licensing agreement) 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; 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 allow the Purchasing Entity to extract its data and the subsequent secure disposal of purchasing entity's data.

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

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

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

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

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

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

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

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum. For commercial available solutions, Access to Security Logs and Reports will be restricted to those that are available with the solution provider's license.

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. Such notifications will not apply to commercially supplied solutions, notifications will be in accordance with the commercial license. Changes will not degrade the terms of services.

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

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

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

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

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

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

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

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

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

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

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

Exhibit 2 to the Master Agreement: Platform-as-a-Service

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

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

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

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement. (Personal data does not include the limited set of data in the Directory which is used to manage user accounts and contains the names and email address of licensed users.)
- 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. (Non-public data does not include the limited set of data in the Directory which is used to manage user accounts and contains the names and email address of licensed users.)
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

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

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

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

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

b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately (or in accordance with a commercial service providers SLA in the licensing agreements) report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

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

a. The Contractor, unless stipulated otherwise, shall immediately (or in accordance with a commercial service providers SLA in the licensing agreement) 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 in accordance with a commercial service providers

SLA in the licensing agreement) or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

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

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

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

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

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

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

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum. For commercial available solutions, Access to Security Logs and Reports will be restricted to those that are available with the solution provider's license.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

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

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a

Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number. Such notifications will not apply to commercially supplied solutions, notifications will be in accordance with the commercial license.

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

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

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

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

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

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

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

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

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

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

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

21. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

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

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

Exhibit 3 to the Master Agreement: Infrastructure-as-a-Service

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

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

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

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement. (Personal data does not include the limited set of data in the Directory which is used to manage user accounts and contains the names and email address of licensed users.)
- 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. (Personal data does not include the limited set of data in the Directory which is used to manage user accounts and contains the names and email address of licensed users.)
- e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

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

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

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach related to Purchasing Entity's Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately (or in accordance with a commercial service providers SLA in the licensing agreement) as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

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

Rationale: Contractor is bound by commercial licenses which define response times to security Incident reporting and data breach notifications which may differ from these clauses.

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA.

a. The Contractor, unless stipulated otherwise, shall immediately (or in accordance with a commercial service providers SLA in the licensing agreement) 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 in accordance with a commercial service providers SLA in the licensing agreement) or sooner by telephone, unless shorter time is required by

applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

Rationale: Contractor is bound by commercial licenses which define response times to personal data breach notifications which may differ from these clauses. Further, it is unreasonable to put a predetermined price on data breaches, the cost should be actual and reasonable damages.

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

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

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

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

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

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

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Contractor directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to in the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Contractor. The report will be sufficient to enable the Purchasing Entity to perform security analysis, resource change tracking and compliance auditing. For commercial available solutions, Access to Security Logs and Reports will be restricted to those that are available with the solution providers license.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

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

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number. Such notifications will not apply to commercially supplied solutions, notifications will be in accordance with the commercial license.

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

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

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

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

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

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

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the

environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime excluding commercially supplied solutions), and provide service to customers as defined in the SLA.

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

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

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

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

Attachment B – Scope of Services

Service Models	Deployment Models			
	Public	Community	Private Off-Premises	Private On-Premises
IaaS	AWS Public	AWS GovCloud Azure Government Cloud ARC-P Community	ARC-P Private	ARC-P On Premise
PaaS	AppWorks	AppWorks ARCWRX	ARCWRX	ARCWRX
SaaS	ServiceNow	Office 365 Microsoft Dynamics CRM Online		

Exhibit 3-1. Service and Deployment Models.

Data risk categories the offeror is capable of storing and securing [5.2.6]

CSRA will store and secure all data risk categories. As documented in the [Exhibit 3-2](#), we offer a full array of options at different data risk levels, which allows our customers to meet the security needs of different applications from a single vendor.

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data
IaaS	AWS Public	AWS GovCloud Azure Government Cloud	ARC-P Community ARC-P Private ARC-P On Prem
PaaS	AppWorks	AppWorks	ARCWRX
SaaS	ServiceNow	Office 365 Microsoft Dynamics CRM Online	

Exhibit 3-2. Identification of Service and Risk Categories

Attachment C – Cost Schedule

Solicitation Number CH16012 NASPO ValuePoint Cloud Solutions RFP

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

Software as a Service	Discount %	<u>1.0%</u>
Infrastructure as a Service	Discount %	<u>1.0%</u>
Platform as a Services	Discount %	<u>1.0%</u>
Value Added Services	Discount %	<u>1.0%</u>

Additional Value Added Services:		
Maintenance Services	Onsite Hourly Rate \$	<u>\$ 81.20</u>
	Remote Hourly Rate \$	<u>\$ 91.73</u>
Professional Services		
• Deployment Services	Onsite Hourly Rate \$	<u>\$ 153.35</u>
	Remote Hourly Rate \$	<u>\$ 173.23</u>
• Consulting/Advisory Services	Onsite Hourly Rate \$	<u>\$ 155.97</u>
	Remote Hourly Rate \$	<u>\$ 176.18</u>
• Architectural Design Services	Onsite Hourly Rate \$	<u>\$ 155.97</u>
	Remote Hourly Rate \$	<u>\$ 176.18</u>
• Statement of Work Services	Onsite Hourly Rate \$	<u>\$ 154.66</u>
	Remote Hourly Rate \$	<u>\$ 174.70</u>
Partner Services	Onsite Hourly Rate \$	<u>\$ 516.11</u>
	Remote Hourly Rate \$	<u>\$ 516.11</u>
Training Deployment Services	Onsite Hourly Rate \$	<u>\$ 77.89</u>
	Remote Hourly Rate \$	<u>\$ 87.98</u>



STATE OF UTAH NASPO VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

VOLUME I: Technical Proposal

UTAH SOLICITATION NO.: CH16012

PREPARED FOR:

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

CSRA POINT OF CONTACT:

David Beach
Advisor, Contracts
(703) 626-9633
David.Beach@csra.com

SUBMITTAL DATE: March 10, 2016

SUBMITTED BY:

CSC State and Local Solutions LLC, A CSRA Company
3170 Fairview Park Drive
Falls Church, VA 22042

FEDERAL TAX IDENTIFICATION NO.: 47-4310550

DUNS NO.: 079735371

Table of Contents

Master Agreement	1
Section 1: RFP Signature Page [3.12 (1), 5.1]	1
Section 2: Executive Summary [3.12 (2), 5.4]	2
Section 3: Mandatory Minimums [3.12 (3)]	5
3.1 Section 3: Cover Letter [5.2]	5
3.2 Acknowledgement of Amendments [5.3]	9
3.3 General Requirements [5.5]	11
3.3.1 Usage Report Administrator [5.5.1]	11
3.3.2 Compliance with NASPO ValuePoint and SciQuest Ordering Instructions [5.5.2]	11
3.3.3 Submission of CSA STAR Registry Self-Assessment [5.5.3]	11
3.3.4 Sample Service Level Agreement (SLA) [5.5.4]	11
3.4 Recertification of Mandatory Minimums and Technical Specifications [5.7]	14
Section 4: Business Profile [6]	15
4.1 Business Profile [6.1]	15
4.2 Scope of Experience [6.2]	19
4.2.1 State of California, California Email Services (CES) [CSC Contract]	20
4.2.2 Federal Aviation Administration (FAA) Cloud Services (FCS) [CSC Contract]	21
4.2.3 Federal Aviation Administration (FAA) Enterprise Messaging System (EMS) [CSC Contract]	25
4.2.4 Department of Justice (DOJ) Drug Enforcement Administration (DEA) Firebird Infrastructure Technology Services (FITS) II [SRA Contract]	28
4.2.5 Department of Health and Human Services (HHS) Health Resources and Services Administration (HRSA) National Practitioner Data Bank (NPDB) [SRA Contract]	30
4.3 Financials (D&B Number) [6.3]	31
4.4 General Information [6.4]	33
4.4.1 Depth and Breadth of Services in the Cloud Marketplace [6.4.1]	33
4.4.2 Auditing Capabilities and Reports [6.4.2]	35
4.5 Billing and Pricing Practices [6.5]	35
4.5.1 Billing and Pricing Practices [6.5.1]	35
4.5.2 Typical Cost Impacts Implementing the Solution [6.5.2]	35
4.5.3 NIST Compliance [6.5.3]	35
4.6 Scope and Variety of Cloud Solutions [6.6]	35
4.7 Best Practices [6.7]	39
Section 5: Organization Profile [7]	41
5.1 Contract Manager [7.1]	43
5.1.1 Contact Information for Contract Manager [7.1.1]	43
5.1.2 Detailed Resume and Description of Contract Manager's Experience [7.1.2]	43
5.1.3 Contract Manager's Roles and Responsibilities [7.1.3]	45
Section 6: Technical Response [3.12 (6), 8]	47
6.1 Technical Requirements [8.1]	50
6.1.1 Identification of Cloud Service and Deployment Model(s) [8.1.1]	50
6.1.2 Meeting NIST Essential Characteristics [8.1.2]	51
6.1.2.1 On-Demand Self Service [8.1.2.1]	51
6.1.2.2 Broad Network Access [8.1.2.2]	51
6.1.2.3 Resource Pooling [8.1.2.3]	51

6.1.2.4	Rapid Elasticity [8.1.2.4]	51
6.1.2.5	Measured Service [8.1.2.5]	51
6.1.3	Identification of Solution Subcategories [8.1.3]	52
6.1.4	Willingness to Comply with Attachments C&D [8.1.4]	52
6.1.5	Offerings Adherence to Attachment D [8.1.5]	52
6.2	Subcontractors [8.2]	54
6.2.1	Intention to Directly Provide Services or through Subcontract [8.2.1]	54
6.2.2	Description of Use of Contractors [8.2.2]	54
6.2.3	Subcontractor Qualifications [8.2.3]	54
6.3	Working with Purchasing Entities [8.3]	55
6.3.1	Working with Purchasing Entities [8.3.1]	55
6.3.1.1	Personnel [8.3.1 bullet 1]	57
6.3.1.2	Response Times [8.3.1 bullet 2]	57
6.3.1.3	Processes and Timelines [8.3.1 bullet 3]	57
6.3.1.4	Communications and Assistance [8.3.1 bullet 4]	58
6.3.1.5	Other Information [8.3.1 bullet 5]	59
6.3.2	Certification of not Pushing Adware, Software or Marketing [8.3.2]	59
6.3.3	Application Hosting and User Test/Staging Environments [8.3.3]	59
6.3.4	Compliance with Accessibility Requirements [8.3.4]	59
6.3.5	Web Accessibility Certification [8.3.5]	59
6.3.6	Purchasing Entity Meeting [8.3.6]	59
6.3.7	Project Schedules and Work Plans	60
6.4	Customer Service [8.4]	60
6.4.1	How Purchasing Entities Provide Customer Service [8.4.1]	62
6.4.1.1	Quality Assurance Measures [8.4.1 bullet 1]	64
6.4.1.2	Problem/Complaint Escalation Plan [8.4.1 bullet 2]	65
6.4.1.3	Service Level Agreements [8.4.1 bullet 3]	66
6.4.2	Compliance with Customer Service Requirements [8.4.2]	67
6.4.2.1	Lead Representative for Each Entity [8.4.2 (a)]	69
6.4.2.2	Availability of Customer Service Representatives [8.4.2 (b)]	69
6.4.2.3	Customer Service Representative Response Time [8.4.2 (c)]	70
6.4.2.4	Design Services [8.4.2 (d)]	71
6.4.2.5	Installation Services [8.4.2 (e)]	71
6.5	Security of Information [8.5]	71
6.5.1	Data Protection [8.5.1]	71
6.5.2	Compliance with Applicable Laws Related to Data Privacy and Security [8.5.2]	74
6.5.3	Plan to Not Access Purchasing Entity's User Accounts [8.5.3]	74
6.6	Privacy and Security [8.6]	75
6.6.1	Compliance with NIST and Other Relevant Standards [8.6.1]	75
6.6.2	Security Certifications Held [8.6.2]	76
6.6.3	Security Practices in Place [8.6.3]	76
6.6.4	Data Confidentiality Standards and Practices in Place [8.6.4]	77
6.6.5	Third-Party Attestations, Reports and Security Credentials [8.6.5]	78
6.6.6	Logging Processes [8.6.7]	78
6.6.7	Restricting Visibility of Cloud Hosted Data and Documents [8.6.7]	78
6.6.8	Security Incident Notification Procedures [8.6.8]	79
6.6.9	Physical and Virtual Zone of Control Security Architectures Security Controls [8.6.9]	79
6.6.10	Security Technical Reference Architectures [8.6.10]	80
6.6.11	Security Procedures for Employees Who Have Access to Sensitive Data [8.6.11]	82
6.6.12	Security Measures and Standards for Data at Rest and In Transit [8.6.12]	83

6.6.13 Policies and Procedures for Notification of a Data Breach [8.6.13].....	83
6.7 Migration and Redeployment Plan [8.7]	84
6.7.1 Maintaining End of Life Activities [8.7.1]	84
6.7.2 Orderly Return of Back Data [8.7.2]	85
6.8 Service or Data Recovery [8.8].....	85
6.8.1 Method of Response [8.8.1].....	85
6.8.1.1 Extended Downtime [8.8.1 (a)]	85
6.8.1.2 Unrecoverable Loss of Data [8.8.1 (b)]	87
6.8.1.3 System Failure [8.8.1 (c)].....	87
6.8.1.4 Recovery and Restoration of Data within Four Business Hours [8.8.1 (d)].....	89
6.8.1.5 Recovery Point Objective (RPO) and Recovery Time Objective (RTO) [8.8.1 (e)].....	89
6.8.2 Methodologies for Backup and Restore Services [8.8.2]	90
6.8.2.1 Data Backups [8.8.2 (a)].....	90
6.8.2.2 Server Image Backups [8.8.2 (b)].....	90
6.8.2.3 Digital Location of Backup Storage [8.8.2 (c)]	90
6.8.2.4 Alternate Data Center Strategies [8.8.2 (d)]	90
6.9 Data Protection [8.9]	91
6.9.1 Standard Encryption Technologies and Options [8.9.1]	91
6.9.2 Willingness to Sign BAA [8.9.2].....	92
6.9.3 Offeror's Use of Data in Master Agreement [8.9.3].....	92
6.10 Service Level Agreements [8.10]	92
6.10.1 Description of SLAs Ability to be Negotiated [8.10.1].....	92
6.10.2 Sample Service Level Agreement (SLA) [8.10.2].....	92
6.11 Data Disposal [8.11]	95
6.12 Performance Measures and Reporting [8.12]	96
6.12.1 Reliability and Uptime Guarantee [8.12.1].....	96
6.12.2 Standard Uptime Service and Related SLA Criteria [8.12.2].....	96
6.12.3 Processes for Call/Contact Support [8.12.3].....	96
6.12.4 Consequences/SLA Remedies for Respondent Failures [8.12.4]	98
6.12.5 Planned Downtime Procedures and Schedules [8.12.6]	98
6.12.6 Consequences/Remedies for not Meeting Recovery Metrics [8.12.7].....	99
6.12.7 Sample Performance Reports [8.12.8].....	99
6.12.8 Printing Historical, Statistical and Usage Reports [8.12.9]	99
6.12.9 24x365 On-Demand Deployment Support [8.12.10].....	99
6.12.10 Description of Scale-Up and Scale-Down Availability [8.12.11]	99
6.13 Cloud Security Alliance [8.13]	100
6.13.1 CSA STAR Self-Assessment [8.13 (a)].....	100
6.13.2 Completion of Exhibits 1 and 2 to Attachment B [8.13 (b)]	100
6.13.3 CSA STAR Registry Attestation, Certification of Assessment [8.13 (c)].....	100
6.13.4 CSA STAR Continuous Monitoring [8.13 (d)]	100
6.14 Service Provisioning [8.14]	101
6.14.1 Processing Emergency or Rush Services Implementation Requests [8.14.1].....	101
6.14.2 Standard Lead-Time for Provisioning the Solution [8.14.2]	101
6.15 Back Up and Disaster Plan [8.15].....	101
6.15.1 Legal Retention Periods and Disposition [8.15.1]	101
6.15.2 Inherent Disaster Recovery Risks and Potential Mitigations [8.15.2].....	102
6.15.3 Infrastructure Supporting Multiple Data Centers [8.15.3].....	102
6.16 Solution Administration [8.16].....	102
6.16.1 Managing Identity and User Accounts [8.16.1].....	103

6.16.2	Providing Anti-Virus Protection [8.16.2]	103
6.16.3	Migrating Data, Metadata and Usage Data [8.16.3]	104
6.16.4	Administering the Solution in a Distributed Manner [8.16.4]	105
6.16.5	Applying Defined Administration Policies [8.16.5]	105
6.17	Hosting and Provisioning [8.17]	105
6.17.1	Cloud Hosting Provisioning Processes and Provisioning Stack [8.17.1]	105
6.17.2	Providing Tool Sets [8.17.2]	105
6.17.2.1	Deploying New Servers [8.17.2.1]	105
6.17.2.2	Creating and Storing Server Images [8.17.2.2]	105
6.17.2.3	Securing Additional Storage Space [8.17.2.3]	106
6.17.2.4	Monitoring Tool Use [8.17.2.4]	106
6.18	Trial and Testing Periods (Pre - and Post - Purchase) [8.18]	106
6.18.1	Testing and Training Periods for Offerings [8.18.1]	106
6.18.2	Providing Test and/or Proof of Concept Environment [8.18.2]	106
6.18.3	No-Cost Training and Support Provided by Offeror [8.18.3]	107
6.19	Integration and Customization [8.19]	107
6.19.1	Integration of Services into Complementary Applications [8.19.1]	107
6.19.2	Customization and Personalization of Services [8.19.2]	107
6.20	Marketing Plan [8.20]	108
6.21	Related Value-Added Services [8.21]	109
6.22	Supporting Infrastructure [8.22]	110
6.22.1	Required Infrastructure [8.22.1]	110
6.22.2	Responsibility for Installation of Infrastructure [8.22.2]	110
6.23	Alignment of Cloud Computing Reference Architecture [8.23]	110
Section 7: Confidential, Protected or Proprietary Information [3.12.7]		112
Section 8: Exceptions and/or Additions to the Standard Terms and Conditions [3.12.8]		113

List of Exhibits

Exhibit 2-1.	CSRA Provides Flexibility, Scalability, and Security.	2
Exhibit 3-1.	Service and Deployment Models.	7
Exhibit 3-2.	Identification of Services per Risk Category.	7
Exhibit 3-3.	Sample SLA.	14
Exhibit 4-1.	CSRA Growth History	16
Exhibit 4-2.	CSRA Retention History	17
Exhibit 4-3.	CSRA Balance Sheet.	33
Exhibit 4-4.	Cloud Migration Services.	34
Exhibit 4-5.	Hybrid Cloud Management.	38
Exhibit 5-1.	Contract Management Approach.	41
Exhibit 5-2.	Contract Support Structure.	42
Exhibit 5-3.	Contract Management Tools and Processes.	43
Exhibit 6-1.	CSRA Concept of Operations.	48
Exhibit 6-2.	Service Categories.	52
Exhibit 6-3.	Incident Response Process.	58
Exhibit 6-4.	Example of Pricing Based on Service Tiers.	62
Exhibit 6-5.	CSRA's Innovative Technology Solution.	64

Exhibit 6-6. Escalation and Notification.....	65
Exhibit 6-7. CSRA’s Technology Solutions.....	69
Exhibit 6-8. CSRA Performance Metrics.....	71
Exhibit 6-9. CSRA’s Layered Security Model.....	76
Exhibit 6-10. ServiceMesh Agility Platform.....	80
Exhibit 6-11. Virtual Disk Snapshot Schedule.....	90
Exhibit 6-12. Sample SLA.....	95
Exhibit 6-13. CSRA’s Solution Set.....	97
Exhibit 6-14. Sample SLA Incentive Plan.....	98
Exhibit 6-15. Azure Performance Report Sample	100
Exhibit 6-16. Marketing Action Plan.....	109
Exhibit 6-17. Patch Management Phase Workflow	109
Exhibit 6-18. The Conceptual Reference Model from the “NIST Cloud Computing Reference Architecture”	111
Exhibit 6-19. Service Model Domains for CSRA Offerings	111

Master Agreement

Section 1: RFP Signature Page [3.12 (1), 5.1]



State of Utah Vendor Information Form

Legal Company Name (include d/b/a if applicable) CSC State and Local Solutions LLC, a CSRA Company		Federal Tax Identification Number 47-3094025		State of Utah Sales Tax ID Number 14024792-002-STC	
Ordering Address 3170 Fairview Park Drive		City Falls Church	State VA	Zip Code 22042	
Remittance Address (if different from ordering address)		City	State	Zip Code	
Type ☐ Proprietorship ☐ Partnership ☐ Government ☒ For-Profit Corporation ☐ Non-Profit Corporation		Company Contact Person David Beach			
Telephone Number (include area code) 703-626-9633		Fax Number (include area code) 410-684-6342			
Company's Internet Web Address csra.com		Email Address david.beach@csra.com			
Offeror's Authorized Representative's Signature 					
Type or Print Name David Beach					
Position or Title of Authorized Representative Advisor, Contracts					
Date: March 10, 2016					

Section 2: Executive Summary [3.12 (2), 5.4]

CSRA's approach to NASPO ValuePoint Cloud Solutions incorporates a breadth of cloud services and technologies that allow us to provide tailored cloud solutions accessible by Participating Entities. We extend the value and usability of our cloud technologies with cloud services that simplify cloud migrations, increase the efficiency of cloud integrations, and leverage managed services to reduce operational costs. Our approach empowers Participating Entities to acquire cloud solutions with appropriate levels of support at a reasonable cost.

CSRA's cloud based services meet essential characteristics

1. On-demand
2. Self-service
3. Broad network access
4. Resource pooling
5. Rapid elasticity
6. Measured service

We team with our strategic alliance partners Microsoft and Amazon to provide Participating Entities a range of cloud service provider (CSP) options, including the following platforms: CSRA's Autonomic Resources Cloud Platform (ARC-P), Microsoft Azure, and Amazon Web Services (AWS). CSRA's strength as a large systems integrator with key strategic CSP alliances allows us to extend alliance discounts to Participating Entities. We complement our CSP offerings with value-added services such as advanced monitoring and migration services that integrate with ARC-P, Azure, and AWS.

Our commercially available infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) and cloud service support services meet the National Institute for Standards and Technology (NIST) definition of cloud computing, and also offer Participating Entities deployment models, security levels, and support services to tailor solutions to meet their specific needs. The range of CSRA's cloud technology offerings allows us to market and respond to Participating Entities needs. We complement implemented technology with technical expertise and exceptional services to Participating Entities.

As a leading systems integrator focused on federal, state and local governments, CSRA offers a variety of cloud computing services designed specifically for government customers. Our initial offering includes ARC-P, AWS, and Azure for IaaS; CSRA's Agility platform for PaaS management; and a variety of SaaS offerings, including a range of Microsoft software suites and ServiceNow. Our cloud offerings are supported by the services depicted in **Exhibit 2-1**:



Exhibit 2-1. CSRA Provides Flexibility, Scalability, and Security. CSRA provides a suite of cloud offerings buoyed by support services.

To improve our offering suite and expand the range of available technologies and services, CSRA constantly surveys the market for cutting-edge cloud solutions at lower costs and with enough maturity to meet the government's needs. As we identify solutions that align with NASPO ValuePoint, we will work with NASPO to add new offerings to this Master Services Agreement (MSA).

To market and promote our NASPO ValuePoint Cloud Services offerings, we capitalize on our outreach capabilities to help Participating Entities understand our cloud technology and service offerings. CSRA's state and local team, led by Vice President of State and Local Andrew Saxe, will market the MSA to states, institutions, and other organizations. Our outreach approach is designed to support the Participating Entity throughout the acquisition process, and inform state governments, agencies, and institutions about the advantages of the NASPO ValuePoint Cloud Solutions vehicle and the suite of CSRA technologies and services that meet the entity's needs and supporting the Participating Entity throughout the acquisition process.

Approach to Providing Cloud Services and Solutions

We meet Participating Entities' objectives through a cost-effective cloud brokering approach implemented in private, public, community or hybrid deployment models, with the opportunity to leverage managed services and tools. CSRA manages uninterrupted cloud brokered operations in cloud environments by translating our experience in systems integration into appropriate application, design and use of best-in-class tools.

The State of California uses CSRA's IaaS, PaaS, SaaS and cloud service support offerings today—we consolidated 80 departments into one cloud email solution. For the city of Los Angeles we migrated 17,000 users from Novell

GroupWise to Google Apps for government; and we provide cloud solutions to federal agencies, including the Department of Defense (DoD), the Federal Aviation Administration (FAA), and the Department of Health and Human Services (DHHS). Our proven approach is also suited to providing NASPO with access to a range of cloud capabilities to state and local governments and agencies.

CSRA's cost-effective cloud brokering business model offers maximum flexibility to help entities meet requirements of varied scope and complexity. As a large systems integrator with key cloud technology channel partnerships, we tailor technology-agnostic approaches to each task order. Our service catalog offers state and local governments access to component and cloud management technologies; deployment and security models; and support services to meet their requirements. Our previous cloud implementations with federal and state government clients give us expertise and lessons learned that Participating Entities can leverage.

CSRA has a performance history delivering data center consolidation and cloud solutions. Our support to the Department of Homeland Security (DHS) Stennis Data Center provides an IaaS and PaaS environment consuming more than 243K virtual CPUs, 883 terabytes of RAM, and 11.7 petabytes of storage daily. We migrated FAA users from a Lotus Notes email application to a cloud-based Microsoft Office 365 environment. CSRA's cloud strategy features offerings from market leaders in addition to emerging technologies through a common, secure, and extensible service delivery platform.

CSRA meets information security requirements by providing a low-risk, flexible, and NIST-compliant architecture. We use a layered security governance process, which assures that we meet state-specific policies and orders. We work with our customers to provide a foundation of continuous monitoring, incident response, disaster recovery and continuity of operations plans.

Flexibility, Scalability and Security

- CSRA provides a range of public and community cloud options, including AWS, Azure and ARC-P private cloud
- We offer a comprehensive suite of technologies supported by expert services capable of meeting the broadest range of state and local government requirements
- *Agility Platform* brokers the use, performance and delivery of cloud services and provides a single user management and operations interface
- Our solutions can fully integrate end-to-end FIPS 140-2 encryption to protect sensitive information

Value-Added Services

To help Participating Entities overcome challenges associated with transitioning to cloud such as migration, user adoption and support, monitoring usage, and optimizing performance, CSRA complements our technical offerings suite with value-added services designed to extend the capabilities, services, and available support models. Our suite of additional services and tools complements our technology offerings to provide automated platform monitoring options, performance analytics tools, and fixed-price migration services that enhance the capability of our cloud technology offerings.

Expanded Support

Our initial offering to NASPO includes offerings from a selected subset of CSRA's partner network. As we expand our support, we will work with other alliance partners to extend their services to Participating Entities via the Cloud Solutions MSA. Our initial offering provides essential cloud services to Participating Entities. We will continue to add future value with service offerings from partner networks such as EMC Networks, AT&T, Brocade Networks, Cloudera, MobileIron, and VMWare. Our commitment to NASPO provides cloud service offerings that meet Participating Entities cloud needs today and in the future. We will work with Participating Entities to shape their enterprises into technology-savvy, cost-effective models.

CSRA Strengths

- Brokerage approach to providing cloud-based technologies meets all requirements, providing an agile framework that allows us to tailor solutions for participating entities and projects of varying size, scope, and complexity
- We extend the value of our offerings with support services ranging from fixed-price migration services to advanced performance analytics tools, which we offer in a leveraged-service model to reduce costs without sacrificing quality or performance
- A durable infrastructure that supports a suite of offerings that includes ServiceNow and Agility
- Our flexible approach is complemented with the tools and support options needed to support cloud service needs in a cost-efficient manner

Section 3: Mandatory Minimums [3.12 (3)]

3.1 SECTION 3: COVER LETTER [5.2]

This page intentionally left blank



March 10, 2016

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

Attn: Christopher Hughes, Assistant Director State of Utah, Division of Purchasing
(christopherhughes@utah.gov)

Reference: NASPO ValuePoint Master Agreement Utah Solicitation Number CH16012 – Cloud Solutions

Dear Mr. Hughes:

CSC State and Local Solutions LLC, a CSRA company (hereinafter and throughout the proposal referred to as CSRA), is pleased to submit its proposal as requested by NASPO ValuePoint Request for Proposal (RFP) Number CH16012. CSC State and Local Solutions LLC's Federal Tax Identification number is 47 3094025 and its Dun and Bradstreet number (DUNS) is 080123603.

Possible requirement to negotiate additional terms and conditions [5.2.1]

CSRA acknowledges that if awarded a contract it may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

Staff responsible for writing the proposal [5.2.2]

CSRA employees were solely responsible for writing this proposal.

Statement offeror is not currently suspended, debarred or otherwise excluded [5.2.3]

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

NASPO ValuePoint Administrative Fee [5.2.4]

CSRA 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.

Service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) [5.2.5]

CSRA acknowledges it is capable of deploying the service model(s) specified in Attachment C and the services models, deployment models and risk categories found in the Scope of Services, Attachment D.

Initially, CSRA will offer the following service models and deployment model combinations. IaaS will be offered in public, community, private off-premises, and private on-premises deployment models. PaaS will be offered in public, community, private off-premises, and private on-premises deployment models. SaaS will be offered in public and community deployment models. **Exhibit 3-1** shows the services currently available in each deployment model.

Service Models	Deployment Models			
	Public	Community	Private Off-Premises	Private On-Premises
IaaS	AWS Public	AWS GovCloud Azure Government Cloud ARC-P Community	ARC-P Private	ARC-P On Premise
PaaS	AppWorks	AppWorks ARCWRX	ARCWRX	ARCWRX
SaaS	ServiceNow	Office 365 Microsoft Dynamics CRM Online		

Exhibit 3-1. Service and Deployment Models.

Data risk categories the offeror is capable of storing and securing [5.2.6]

CSRA will store and secure all data risk categories. As documented in the [Exhibit 3-2](#), we offer a full array of options at different data risk levels, which allows our customers to meet the security needs of different applications from a single vendor.

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data
IaaS	AWS Public	AWS GovCloud Azure Government Cloud	ARC-P Community ARC-P Private ARC-P On Prem
PaaS	AppWorks	AppWorks	ARCWRX
SaaS	ServiceNow	Office 365 Microsoft Dynamics CRM Online	

Exhibit 3-2. Identification of Services per Risk Category.

Points of Contact

The individuals listed below are authorized to negotiate on behalf of CSRA.

Name	Phone	Fax	E-mail
David Beach, Advisor, Contracts	(703) 626-9633	(410) 684-6342	david.beach@csra.com
Raymond Glass Manager, Contracts & Commercial Management	(410) 872-7868	(410) 684-6342	raymond.glass@csra.com

On August 31, 2015, CSC and SRA announced that they had entered into a definitive agreement to combine the business operations of Computer Sciences Corporation's government services unit, CSC Government Solutions, LLC, and its subsidiaries (CSGov), and SRA International, Inc., to form a new family of companies under a common, publicly traded parent company, CSRA Inc.

The transaction closed on November 30, and SRA and CSGov are now operating as sister companies under CSRA. Both SRA and CSGov are providing all necessary notifications regarding ownership and operating status to the government, in accordance with the Federal Acquisition Regulation. Following the May 2015 announcement by CSC that its North American Public Sector business would become CSGov, the government approved a conversion and change of name agreement effective July 4, 2015. At this

time, SRA and CSGov continue to operate as separate, subsidiaries of CSRA Inc., and will continue to maintain their approved procedures, processes and business systems.

The CSRA companies are committed to making a difference supporting the government as it serves our country and our citizens. Our 19,000 employees work together to deliver solutions and services to enable the safety, security, health and well-being of our nation. We continue to deliver a broad range of innovative, next-generation IT solutions and professional services to help our customers modernize their legacy systems, protect their networks and assets, and improve the effectiveness and efficiency of mission-critical functions.

While we merge our companies, we assure you that our priority is to provide outstanding support and maintain continuity among our program/project teams.

Sincerely,

A handwritten signature in black ink, appearing to read "D. Beach", written in a cursive style.

David Beach
Advisor, Contracts
7231 Parkway Drive
Hanover, MD 21076
(703) 626-9633

3.2 ACKNOWLEDGEMENT OF AMENDMENTS [5.3]

CSRA 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.

First Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the first amendment document posted on December 22, 2015, 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.

__ CSC State and Local Solutions LLC, a CSRA company _____
Offeror

 _____

Second Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the second amendment document posted on December 24, 2015, 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.

__ CSC State and Local Solutions LLC, a CSRA company _____
Offeror

 _____

Third Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the third amendment document posted on January 5, 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.

__ CSC State and Local Solutions LLC, a CSRA company _____
Offeror

 _____

Fourth Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the fourth amendment document posted on January 12, 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.

__ CSC State and Local Solutions LLC, a CSRA company _____
Offeror

 _____

Fifth Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the fifth amendment document posted on January 15, 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.

__ CSC State and Local Solutions LLC, a CSRA company _____

Offeror



Sixth Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the sixth amendment document posted on January 28, 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.

__ CSC State and Local Solutions LLC, a CSRA company _____

Offeror



Seventh Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the seventh amendment document posted on February 1, 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.

__ CSC State and Local Solutions LLC, a CSRA company _____

Offeror



Eighth Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the eighth amendment 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.

__ CSC State and Local Solutions LLC, a CSRA company _____

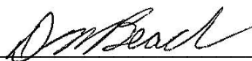
Offeror



Ninth Amendment

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the ninth amendment document posted on February 5, 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.

__ CSC State and Local Solutions LLC, a CSRA company _____
Offeror

 _____

Tenth Amendment

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

__ CSC State and Local Solutions LLC, a CSRA company _____
Offeror

 _____

Final RFP

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.

__ CSC State and Local Solutions LLC, a CSRA company _____
Offeror

 _____

Representative Signature

3.3 GENERAL REQUIREMENTS [5.5]**3.3.1 Usage Report Administrator [5.5.1]**

Upon contract award, CSRA certifies it will provide a Usage Report Administrator.

3.3.2 Compliance with NASPO ValuePoint and SciQuest Ordering Instructions [5.5.2]

CSRA agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading ordering instructions.

3.3.3 Submission of CSA STAR Registry Self-Assessment [5.5.3]

CSRA's vendors maintain current CSA STAR Registry Self-Assessments. We have included completed Consensus Assessments Initiative Questionnaires (CAIQ) and Cloud Controls Matrixes (CCM) from our vendors as attachments to this proposal. Attachments 1 - 7 can be found in Volume 1 Attachments. CSRA warrants that the vendors have completed these with accuracy and currency to the best of CSRA's knowledge.

3.3.4 Sample Service Level Agreement (SLA) [5.5.4]

Response time SLAs (otherwise known as "Time to Respond", which does not include resolution) assures that all clients are entitled to reimbursement of 1/30th of their applicable monthly recurring charges for

any calendar month in which CSRA fails to notify or respond to events within the timeframes outlined in the schedule below.

For purposes of this SLA, the terms notify, respond, and mean time are defined as:

- **Notify:** CSRA will call back or respond electronically to the designated client contact
- **Respond:** CSRA will begin working on the problem and/or ticket item
- **Mean Time:** arithmetic mean; all occurrences for a severity level will be averaged over a calendar month

Service Levels for AWS and Azure

Entities purchasing AWS or Azure services are entitled to the Service Levels described on their respective web site. CSRA will extend Microsoft and AWS' existing SLA structure to Purchasing Entities (see <http://aws.amazon.com/ec2/sla/> or <http://azure.microsoft.com/en-us/support/legal/sla/> for the current version of these SLAs). **Exhibit 3-3** is a sample of ITSM SLAs.

Service Category & SLA Description	Descriptions	Performance Standard
Service Desk		
Average Speed to Answer (ASA)	Response Time for EMOC to answer	<60 Sec Avg
Status Update Frequency	EMOC Tickets updated daily	90%
Customer Satisfaction Rating	Mean of Survey Averages per Quarter	3.5 score on scale of 1 to 5
Incident Management		
Resolution Time	% of Incidents meeting the Hourly Target Duration for respective Severity level	90% for all
Severity 1	<4 Clk Hrs	
Severity 2	<8 Clk Hrs	
Severity 3	<16 Bus Hrs	
Severity 4	<24 Bus Hrs	
Incident Management		
Time for customer to be notified when non security incident is found	Error Rate for those occurring after 1 Hr	10%
Service Asset and Configuration Management		
Percent accuracy of key fields for CIs in CMDB of level 2-3 systems - 20% minimum per month sample	% of fields per CI of audited sample having error; Monthly	5%
Hardware assets inventoried - Level 1-3 systems - minimum 10% monthly sample	Annual; 100% concurrence of audits done monthly	100%
Software assets inventoried - Level 2-3 systems - minimum 10% monthly sample	Annual; 100% concurrence of audits done monthly	100%
Change Management		
Percent of successful implemented changes - Level 2 and 3	% of successful changes	80%
Percent of changes resulting in an incident	% of changes resulting in an incident	10%
Percent of Emergency Changes	% of emergency changes	<20%
Percent of Backed Out Changes	% of backed out changes	<20%
Release and Deployment Management		
Successful release percentage - Major	% of successful releases	80%
Successful release percentage - Minor	% of successful releases	80%
Successful release percentage - Emergency	% of successful releases	80%

Service Category & SLA Description	Descriptions	Performance Standard
Availability Management		
Percentage of System Availability - Level 2-3 Systems	Total System Hrs	99.90%
Percentage of LAN Availability	by total LAN Hrs	99%
Capacity Management		
% of CPU utilization - Level 2 and 3 systems - Enterprise	Monthly; Avg % of CPU Utilization of CSRA L2/3 supported DHS systems; Enterprise view	80%
% of Disk utilization - Level 2 and 3 systems - Enterprise	Monthly; Avg % of Disk Utilization of CSRA L2/3 supported DHS systems; Enterprise view	80%
% of SAN utilization - Level 2 and 3 systems - Enterprise	Monthly; Avg % of SAN Utilization of CSRA L2/3 supported DHS systems; Enterprise view	80%
% of Network Bandwidth utilization	Monthly; Avg % of Bandwidth Utilization of CSRA supported DHS DC1 Network Switches for LAN/WAN; Enterprise view	80%
IT Service Continuity Management		
Monthly Backup Success Rate Average	Monthly; % of Backups Not Having a Client failure 2 days in a row	98%
% of funded clients having DR plan documented	Annual; DR Funded Clients	100%
% Successful System Recovery Testing	Annual; System Recovery Tests performed	90%
% Successful LAN Recovery Testing	Annual; DC1 LAN Recovery Tests performed	90%
% Audits and Reviews of DR Plans Completed	Annual; DR Funded Clients' Plans Reviewed	100%
DR Level 1 - No DR		
DR Level 2 - >=30 days	Annual; % Testing Recoverable w/in threshold	100%
DR Level 3 - within 30 days	Annual; % Testing Recoverable w/in threshold	100%
DR Level 4 - within 8 days	Annual; % Testing Recoverable w/in threshold	100%
DR Level 5 - within 24 Hrs	Annual; % Testing Recoverable w/in threshold	100%
DR Level 6 - within 8 Hrs	Annual; % Testing Recoverable w/in threshold	100%
DR Level 7 - within 4 Hrs	Annual; % Testing Recoverable w/in threshold	100%
DR Level 8 - Active, Active - Complete failover and near zero recovery time and recovery point	Annual; % Testing Recoverable w/in threshold	100%
Additional - Available for Use One year after Contract		
Information Security Management		
Security Intrusion Detection	% of Intrusion Detections Captured by intrusion detection system (IDS) Sensors	95%
Security Intrusion Reporting and Compliance	% of "significant" Incidents reported within 1hr	95%

Service Category & SLA Description	Descriptions	Performance Standard
Access Termination	% of terminated employees with access removed	95%
Vulnerability Scan Compliance - Level 3	% of Level 3 systems having no “high” vulnerabilities listed or are within the Comply Date posted	95%
Certification and Accreditation Compliance	% of systems/apps having full C&A support from CSRA with unexpired ATO	95%
Virus Protection Management Compliance to Standard - Level 2 - Wintel	% of Level 2 CSRA supported Wintel servers having Antivirus signatures newer than 5 days	95%
Information Security Awareness Training Compliance	% of CSRA employees having received Security Awareness Training	95%

Exhibit 3-3. Sample SLA. A sample of ITSM SLA’s are provided here for reference.

3.4 RECERTIFICATION OF MANDATORY MINIMUMS AND TECHNICAL SPECIFICATIONS [5.7]

The assigned CSRA Contract Manager will annually recertify with the Lead State that we meet or exceed the mandatory minimum requirements of this RFP.

Section 4: Business Profile [6]

4.1 BUSINESS PROFILE [6.1]

Year Started

We began assisting our government clients migrating to the cloud with our first cloud contract award in 2009. At the time of award, CSRA operated as the CSC North American Public Sector. CSC has worked for the government for more than 50 years; we formed the federal sector division to focus on government work. Since then, CSC North America spun off and formed CSRA, the largest pure-play government IT contractor, in November 2015 through the combination of the former CSC North American Public Sector—now CSC Government Solutions, LLC (CSGov)—and SRA International. With more than 90 years of combined experience supporting state, local, and federal government agencies and programs, we help the government serve our country and citizens.

CSRA's Organizational Structure

CSRA, headquartered in Falls Church, Virginia, delivers offerings from concept through sustainment. Following consummation of the mergers, with the inclusion of SRA, we employ approximately 19,000 employees. We manage our business with a matrix model comprising customer-facing industry verticals with knowledge of our customers' missions, and a horizontal delivery organization with technical expertise that it delivers across industries. We operate in two industry verticals, Defense and Intelligence, and Civil, which also serve as our reportable segments.

Delivery and Operations, our horizontal delivery organization, provides capabilities and solutions across our customer base. We differentiate ourselves by combining our technical expertise in applications and IT infrastructure solutions with our public sector mission experience to engage our customers with thought leadership that drives change.

Our two reportable segments are our industry verticals:

- Defense and Intelligence—The Defense and Intelligence segment provides services to the Department of Defense, National Security Agency, and branches of the Armed Forces.
- Civil—The Civil segment provides services to federal agencies within the Department of Homeland Security, the Department of Health and Human Services, other federal civil agencies, and state and local government agencies.

CSRA's Client Base

CSRA has expanded its leadership role in the Cloud Services market by partnering with myriad cloud service providers (CSPs) and data center colocation providers, such as Amazon Web Services (AWS), Microsoft (Azure and Office 365), Google, Equinix, CentreTEK, Minburn, KeyBridge, ICS, and Cloudnexus. We developed offerings such as BizCloud for Government and our Agility Platform to offer our clients flexible, cost-effective solutions. Our Agility Platform provides a unified interface for app and data portability, operational and development configuration management, and changes based on client policies and procedures. Our price arbitrage of cloud services implemented through Agility Platform's brokering capabilities provides an open application programming interface (API) architecture and extensible meta model for our clients to exploit IaaS, PaaS, and SaaS requirements of Federal Risk and Authorization Management Program (FedRAMP) service providers at the best price.

CSRA has delivered on-schedule, on-budget, and quality infrastructure and end user services to our federal, state, and local customers for more than 50 years. Gartner, Inc. rated us as the sole company in the Leader (Magic) Quadrant for IaaS¹ and End-User Outsourcing Services² in 2013. CSRA's enterprise alliance with Amazon unites the only two companies in Gartner's 2013 Magic Quadrant for Cloud IaaS report to accelerate the development of cloud solutions for enterprise and public sector customers. Amazon has qualified CSRA, an authorized AWS reseller, as an AWS Advanced Consulting Partner and an AWS Premier Consulting Partner, which allows us to offer the largest discounts for AWS services.

CSRA's Three Year Growth Rate in the Cloud Services Space

CSRA presents a combined annual revenue and head count that incorporates CSGov and SRA figures to demonstrate three years of growth history. CSGov's fiscal year lasts from April to March and SRA's lasts from July to June. We generated the combined reporting using each company's fiscal year records. As prime contractors focused on providing IT services to federal, state, and local customers, CSGov and SRA have experienced reduction in revenue due to industrywide budget pressures from sequestration, decline in mission support to overseas contingency operations (OCO), and the divestiture of noncore assets. CSRA concentrates our focus in IT. With over three-quarters of our staff dedicated to IT, our total company metrics serve as the basis for our growth and retention statistics. **Exhibit 4-1** shows our revenue and head count over the last three years.

Metric	FY13	FY14	FY15	FY13-FY15
CSRA Revenue (M)	\$6,170	\$5,485	\$5,446	N/A
Revenue Growth (M)	N/A	-\$685	-\$39	-\$724
Growth Rate	N/A	-11.1%	-0.7%	-3.9%
CSRA Headcount	19,395	19,596	19,145	N/A

Exhibit 4-1. CSRA Growth History

CSRA's Number of Employees

Our 19,000 employees remain focused on our customers and demonstrate ethical leadership and commitment to excellence in program execution. We aspire to achieve great feats for our customers and aim to deliver results to help them succeed. Our teams collaborate with our customers and business partners to deliver the best technologies and solutions aligned to mission requirements.

CSRA's Retention Rate for Our Cloud Services Employees

CSRA presents voluntary attrition figures for CSGov and SRA when they operated as independent companies to demonstrate two years of retention history. As prime contractors focused on providing IT services to federal, state, and local customers, CSGov and SRA general retention and attrition rates represent the employees associated with the services our NASPO ValuePoint Cloud Solutions MSA provides.

CSRA has demonstrated an ability to retain our most highly qualified personnel, driven by growing opportunities in next generation IT.

Company	FY14	FY15
CSGov Voluntary Retention Rate	80.1%	81.4%
SRA Voluntary Retention Rate	82.6%	82.6%

Exhibit 4-2 shows our retention rate for the last two years.

¹ Gartner: Magic Quadrant for Cloud Infrastructure as a Service
<http://www.gartner.com/technology/reprints.do?id=1-115JDYG&ct=130805&st=sb>

² Gartner: Magic Quadrant for End-User Outsourcing Services, North America
<http://www.gartner.com/technology/reprints.do?id=1-115JDYJ&ct=130805&st=sb>

Company	FY14	FY15
CSGov Voluntary Retention Rate	80.1%	81.4%
SRA Voluntary Retention Rate	82.6%	82.6%

Exhibit 4-2. CSRA Retention History

CSRA's Corporate Experience Delivering Cloud Solutions for Large Scale Projects

In addition to the five contracts in the next section, the table below provides a representative sample of our experience in cloud solutions within the last three years. It covers a range of clients (state, local, and federal), and summarizes the cloud solutions provided and their large-scale complexity. It contains examples from both of CSRA's legacy companies (CSC and SRA), and retains those names because they are the legal entities on the contracts with those respective agencies.

Contract Name: State of California California Email Services (CES)	Cloud Solutions Provided: Infrastructure as a Service (IaaS) Software as a Service (SaaS) Email as a Service (EaaS)
Years of Experience: 2010 – 2015	
Large-Scale Complexity: CSC provided Microsoft Cloud Services in a secure cloud environment, offering comprehensive email and legal eDiscovery services and collaboration tools for mobile users. CSC also provided migration services to the new cloud solution and standardized email across all state agencies that selected the service, potentially eliminating up to 130 email systems using three different email platforms. The Microsoft Cloud Services improved data security, simplified email administration, enhanced agency collaboration, and improved responsiveness to public information requests.	
Contract Name: City of Los Angeles Software as a Service (SaaS) E-Mail & Collaboration Services (SECS)	Cloud Solutions Provided: Infrastructure as a Service (IaaS) Software as a Service (SaaS) Platform as a Service (PaaS) Email as a Service (EaaS) SAP as a Service Business Process as a Service
Years of Experience: 2009 – 2014	
Large-Scale Complexity: The City of Los Angeles partnered with CSC and Google to develop a real-time document-sharing capability offering robust security protection. The solution was founded on CSC's Trusted Cloud Computing and Google's email program (Gmail). CSC provided cloud orchestration services and implemented the Google Apps for Government suite of Web-based productivity tools, while making available mission-critical communication and collaboration capabilities to more than 17,000 employees of the City of Los Angeles. Google Apps for Government provided segregated systems for US Government customers in a secure public cloud environment. With Google, CSC provided cutting-edge technology services with a scope that covered areas such as infrastructure, IT systems, and cross-cutting activities. CSC provided migration services for mailbox data migrating from Novell GroupWise to Google Apps. Across more than 36 city departments, CSC supplied migration scripts to migrate mailboxes, calendar items, contacts, and distribution lists. CSC furnished dedicated project management and management support to the city. This solution expects to save the City of Los Angeles \$5.5 million over five years.	
Contract Name: Department of Health and Human Services (HHS) Health Resources and Services Administration (HRSA) National Practitioner Data Bank (NPDB)	Cloud Solutions Provided: Infrastructure as a Service (IaaS) Cloud Computing Cloud Architecture
Years of Experience: 2012 – 2016	
Large-Scale Complexity: Since 1994, SRA has held the HHS contract to design, develop, engineer, implement, enhance, maintain, and operate the NPDB, a national clearinghouse to collect and release information related to the professional competence and conduct of health care practitioners. The NPDB processes more than 4.6 million transactions per year (about 89,000 per week) for more than 46,000 registered users on more than 1.2 million adverse action reports on 625,000 healthcare practitioners. It also processes practitioner self-queries for an estimated 75,000 physicians and dentists. NPDB generates a total of about \$25 million annually for the	

government through its online fee-for-service e-commerce model. HSRA wanted to reduce costs related to hardware, software, hosting, and other operational costs. SRA conducted a trade study to evaluate potential Infrastructure as a Service (IaaS) vendors, focusing on technical capability, cost, and security. Based on our proof-of-concept prototype, we successfully migrated the full NPDB system to the cloud in November 2014. SRA delivered all generations of the NPDB system on schedule and within budget. Since migrating the NPDB application and data to Amazon Web Services (AWS), SRA has helped HSRA reduce its system operating costs by \$80,000 per month, while boosting self-service activity by streamlining credit purchasing processes and fees.	
Contract Name: US Army ITES-2S, Software Engineering Center (SEC) Architecture Services Division (ASD) Software Development Support Services	Cloud Solutions Provided: Infrastructure as a Service (IaaS) Software as a Service (SaaS) Platform as a Service (PaaS) Email as a Service (EaaS) SAP as a Service Business Process as a Service
Years of Experience: 2011 – 2013	
Large-Scale Complexity: CSC provided program management, systems engineering, information assurance, business process engineering, biometrics integration, SOA/Enterprise Resource Planning (ERP)/business intelligence, cloud computing, enterprise resource planning, service-oriented architectures, virtualization, software requirements engineering, software design, full lifecycle software development/management, software/systems testing, software maintenance, configuration management, software engineering management, systems modeling, network infrastructure assistance, business intelligence, enterprise data management, enterprise data warehousing, emerging technologies and Enterprise Integration Business Environment (EIBE) design, development and maintenance.	
Contract Name: Environmental Protection Agency (EPA) Office of Transportation and Air Quality (OTAQ) Compliance (Verify)	Cloud Solutions Provided: Infrastructure as a Service (IaaS) Platform as a Service (PaaS) Development/Test as a Service (DTaaS)
Years of Experience: 2009 – 2015	
Large-Scale Complexity: EPA's engine and vehicle compliance information system, Verify, collects emissions and fuel economy compliance information from engine and vehicle manufacturers for various types of engines, vehicles, and equipment used in transportation and other mobile source applications. Verify, a five-year effort valued at more than \$23M, provided consulting services, system development, maintenance, configuration management, and data support to users in the Washington, D.C. area and EPA offices around the country. Using AWS, CSC implemented IaaS and PaaS in a private cloud environment to provide Verify Cloud, which supports Development/ Test as a Service (DTaaS). The environment comprises three instances of public-facing extranet and a private intranet, each of which uses an Oracle database as a data repository. In addition, the cloud hosts the build and deployment server. We provide a cloud environment for the development and test environments for the EPA Verify information system.	
Contract Name: Administrative Office of US Courts (AOUSC) US Courts Judiciary Data Center (JDC) Infrastructure Support	Cloud Solutions Provided: Cloud Architecture Cloud Virtualization Infrastructure as a Service (IaaS) Platform as a Service (PaaS) Software as Service (SaaS)
Years of Experience: 2009 – 2016	
Large-Scale Complexity: SRA supports Administrative Office of the US Courts (AO) Cloud Technology and Hosting Office (CTHO), which provides infrastructure, platform, and storage services for applications that support business functions of the AO, Federal Courts, and other offices of the Federal Judiciary by providing expertise in a variety of technical disciplines, including virtualization architecture, design, and implementation; storage engineering; systems administration; network engineering and administration; and database administration. SRA's team supports AO's requirements for hosted service delivery that comprise Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) technologies nationwide to the Federal Judiciary. SRA administers more than 900 servers supporting 32,000 users in more than 800 locations nationwide.	

Contract Name: US Agency for International Development (USAID) USAID IT Forward — Top Level	Cloud Solutions Provided: Cloud Computing Mobile Computing Virtualization Infrastructure as a Service (IaaS) Software as a Service (SaaS)
Years of Experience: 2012 – 2017	
Large-Scale Complexity: The USAID worldwide network supports approximately 11,000 network users in 90 locations around the world. Approximately 3,000 users reside in the Washington, D.C. metropolitan area with links to six Metropolitan Area Network (MAN) sites, with plans to add a seventh node to the environment. The remaining 8,000 network users reside in 90 missions throughout the developing world. All missions connect back through Washington via the Wide Area Network (WAN). Also, VPN connections remain in place between many missions to enable direct access for applications and file sharing. The network uses Cisco switches and routers and maintains a strong security perimeter with Juniper firewalls and Blue Coat network devices installed in all locations. CSC helps USAID to migrate these standalone servers to a virtual environment using VMWare ESX. We actively leverage new technologies in this effort, such as Google applications, Virtual Desktop Infrastructure (VDI), and server virtualization, while moving the data center to a third-party hosting facility, and incorporating wireless networking and mobile application access. This will result in a more cost-effective and secure mobile computing environment that will increase data access capabilities and improve communications throughout the agency and with external development partners.	
Contract Name: General Services Administration (GSA) IT Schedule 70, Email as a Service (EaaS) (Microsoft Solution)	Cloud Solutions Provided: Software as a Service (SaaS) Email as a Service (EaaS) Government Community Cloud Private Cloud Secret Enclave Private Cloud Public Cloud
Years of Experience: 2012 – 2017	
Large-Scale Complexity: CSC provides SaaS offerings to the government, available within a Government Community Cloud, Provider Furnished Equipment Private Cloud, Secret Enclave Private Cloud, and Public Cloud deployment model — Email-as-a-Service (EaaS), Office Automation Software-as-a-Service (to support additional functionality that interoperates with the EaaS offerings), the Electronic Records Management Software-as-a-Service (to support the EaaS offerings), migration services (to transition data to and from the EaaS offerings), and integration services.	
Contract Name: Federal Aviation Administration (FAA) Enterprise Messaging System (EMS)	Cloud Solutions Provided: Software as a Service (SaaS) Email as a Service (EaaS) EaaS Implementation
Years of Experience: 2012 – 2019	
Large-Scale Complexity: CSC’s work under this contract supports the FAA’s efforts to transition from legacy client-server based messaging solutions to a 508-compliant cloud messaging service that allows access to data anywhere, anytime, through a full spectrum of devices. The seven-year effort includes 18 FTEs and provides support to 60,000 desktop and laptop users, 20,000 Internet access-only users, and 30,000 mobile devices including thick and thin clients, smartphones, and tablets with high-availability service. The FAA service is Dedicated D-ITAR (International Traffic in Arms Regulations), which requires more capacity planning and higher security features than Government Community Cloud.	

4.2 SCOPE OF EXPERIENCE [6.2]

In November 2015, Computer Science Corporation’s (CSC) North American Public Sector business and SRA International merged to form CSRA, a large systems integrator focused solely on supporting the public sector. CSRA has earned recognition as a leader in technology-enabled business solutions and services for government customers. Our corporate experience and qualifications provide a significant resource base to effectively and efficiently support NASPO ValuePoint, state governments, institutions,

and organizations' business objectives with high-quality services, exceptional performance, and targeted innovation.

Our selected Scope of Experience references will include projects awarded to both CSC and SRA when they operated as independent companies. CSRA now incorporates the full scope of each referenced task with full responsibility and accountability for their continued success.

Detailed Description of Business Experience [6.2]

The following five past performance references represent the five largest contracts within the last two years from CSRA in cloud computing. The past performance references include varied contract types for both state and federal clients, including Indefinite Delivery Indefinite Quantity (IDIQ) with multiple task orders (TOs), GWACS, full and open vehicles, and TOs. These contracts range from our clients' early forays into cloud computing, which shows how we championed cloud technology from its inception, to our clients' more current contracts that show how cloud procurement and solutions have evolved.

These contracts support the Master Agreements for NASPO ValuePoint by:

- Providing cloud solutions to a variety of environments
- Providing a menu of cloud solutions to increase operational efficiencies, reduce cost, enhance operational scalability, and ensure business continuity while improving collaboration and expanding flexible work practices
- Meeting NIST essential characteristics in one or more service models (SaaS, PaaS, and IaaS)

4.2.1 State of California, California Email Services (CES) [CSC Contract]

Agency:	State of California
Contract Full Name:	California Email Services
Contract Short Name:	CES
Contract Number:	09-120431
Contract Type:	Time & Materials (T&M) and Firm Fixed Price (FFP)
Period of Performance:	10/13/2010 to 10/12/2015
Total Contract Value:	\$73,255,951
Overview/Scope of Work:	
Work under this contract supports California's efforts to improve information technology (IT) infrastructure, increase government efficiency, save costs, and consolidate IT functions under the Office of the State Chief Information Officer. The California Email Service (CES), a five-year effort valued at more than \$74 million, included 12 full-time equivalents (FTEs) plus subcontractors, and provided support to up to 90,000 users. CSC provided Microsoft Cloud Services in a secure cloud environment, offering comprehensive email and legal eDiscovery services and collaboration tools for mobile users. CSC also provided migration services to the new cloud solution and standardized email across all state agencies that selected the service. CSC partnered with Microsoft as one of a limited number of global resellers of the Microsoft Office 365 suite (formerly called Business Productivity Online Suite-Dedicated). CSC is the only authorized Microsoft Office 365 public sector reseller that also serves as a global systems integrator. CSC is also the only systems integrator/reseller that has implemented Microsoft Office 365 for a large, complex public sector entity.	
Categorization of Risk:	
☒ Low Risk Data ☐ Moderate Risk Data ☐ High Risk Data	
How Contract Meets Five Essential Characteristics of a Cloud-Based Service Model:	
On-Demand Self-Service: The client's email administrators can unilaterally provision new email user accounts without the assistance of CSC or Microsoft and can adjust their storage needs as required. Broad Network Access: CES users can access email services through Microsoft Outlook on their desktop workstations and Outlook Web Access (OWA) online through the Web or over mobile devices.	

Resource Pooling: The service is designed as a multi-tenant model where various state agencies have the option to subscribe or remain on their legacy systems. The solution also supports sharing and delegation of address lists, mailboxes, and calendars.

Rapid Elasticity: The system can scale rapidly on demand to accommodate individual new-user additions or state agencies that decide to subscribe to the service.

Measured Service: Our email solution allowed users to select from three different mailbox capacities: 500MB, 5GB, or 25GB. The client can also monitor, control, and report resource usage.

Cloud-Based Service Models Used In This Contract:

Infrastructure as a Service (IaaS): CSC worked with Microsoft to deploy an IaaS cloud solution encompassing three different platforms plus online environments to provide comprehensive email and collaboration services to public employees of the US's most populous state. This solution standardized email across California and eliminated up to 130 legacy email systems. The Microsoft Cloud Services IaaS improved data security, simplified email administration, enhanced agency collaboration, and improved responsiveness to public information requests.

Software as a Service (SaaS): The CES platform provides software in an integrated Microsoft Office 365 Dedicated (Office 365-D) cloud implementation with Microsoft Exchange, Microsoft SharePoint, Microsoft Office Communicator, Proofpoint Data Archival and E-Discovery, and Microsoft Live Meeting, and collaboration tools for mobile users.

Email as a Service (EaaS): State users access email, calendar, and contact tasks through Active Directory authentication. The Microsoft Office 365 solution supports two-factor authentication. State customers subscribing to our solution can use Swivel PINSafe or RSA SecurID two-factor authentication methods implemented to authenticate to messaging resources exposed with Outlook Web Access (OWA). CSC also provided integration with the on-premise State Active Directory and more than 70 Active Directory forests. Through Enterprise Active Sync (EAS) support, the state can enforce policies for Active Sync devices such as Blackberry, Android, and iPhone. We also built instant messaging capability into the system and included outside IM addresses through providers such as AOL, MSN, and Yahoo. Microsoft Office Communications Online (OCO) and LiveMeeting supported the ability to share desktop and applications. Microsoft Office 365 offers integrated presence status updates, including Online, Away, Busy, Do Not Disturb, and Offline. OCO provided the state with integrated presence and real-time communications services including instant messaging and PC-to-PC audio and video communication.

Deployment Method:

☐ Private Cloud ☐ Community Cloud ☐ Public Cloud ☒ Hybrid Cloud

Accomplishments/Customer Feedback:

On a recent Customer Satisfaction Survey, the state government customer rated CSC in the following areas:

When responding to "CSC offers solutions that match your needs," users rated CES as 8.25 (out of 10)

When responding to "CSC delivers exceptional service," we received an 8.75 rating.

When responding to "CSC is proactive in addressing your needs," we received a 9 rating. Our customer noted that "the program director, PMs, and technical staffs are very knowledgeable and professional..."

When responding to "CSC understands your business needs," we received another 9 rating.

When responding to "CSC brings you the benefits of its global scale and capability," the government customer rated CES as 8.5.

As part of a contract extension, CSC negotiated a significant reduction of the monthly fees for the service, saving the State over \$3M per year.

4.2.2 Federal Aviation Administration (FAA) Cloud Services (FCS) [CSC Contract]

Agency:	Federal Aviation Administration (FAA)
Contract Full Name:	FAA Cloud Services (FCS)
Contract Short Name:	FAA FCS
Contract Number:	DTFAC-15-D-00003
Contract Type:	IDIQ with FFP and T&M
Period of Performance:	08/26/2015 to 08/25/2025

Total Contract Value:	\$108,922,884
Overview/Scope of Work:	
The FAA sought to acquire co-location and cloud computing services to consolidate its 152 data centers and replace aging legacy infrastructure that currently supports a diversified user community. The FAA wanted to reduce costs while providing high availability and reliability to the National Airspace System (NAS), Mission, and Administrative user communities. CSC's solution consolidates existing IT infrastructure into a flexible and secure FedRAMP certified cloud hosted environment with additional FAA security controls. We completed this type of work for DHS, HHS, TSA, and many other federal and defense customers. On another FAA contract (FAA EMS365), we partnered and worked closely with FAA leadership to plan and manage program execution while facilitating effective communications and collaboration. Our lessons learned on that program made CSC well-suited to merge our technical and domain expertise to deliver success on FCS. We provided a cost-effective cloud brokering business model, implemented it in a secure hybrid cloud services environment, and monitored and managed it with our Agility Platform. Our FCS solution united CSC's BizCloud for Government with AWS- and Microsoft Azure FedRAMP-certified Cloud offerings. This allows us to drive value for the FAA by fostering Cloud Service Provider (CSP) price competition using this competitive cloud brokering approach. CSC's cloud services solution leverages: • Our global experience as a Tier III and data center provider. • Our strategic partnership with Equinix, a data center co-location services provider. • Our proven teammates and technology partners to support and lead the FAA through its planned data center consolidation and cloud migration to the objective state environment. We intend to bring the experience and expertise gained through work completed on FAA EMS365 and DHS Stennis DC1. • Our expansive network of strategic global alliances with AWS, Microsoft, VMware, EMC, IBM, Oracle and many other technology leading firms. • Our FedRAMP-certified CSPs in AWS and Microsoft Azure. • Our Team CSC partners such as Amazon, Microsoft, Equinix, CentreTEK, Minburn, KeyBridge, ICS, and Cloudnexus. • Our hybrid cloud management approach with unifying features such as security and performance monitoring, metering and chargeback, authentication and access controls, orchestration of policies and lifecycle event management across cloud providers and platforms. • Our Information Technology Service Management (ITSM) and security operations center (SOC) services supporting the FAA SLA and reporting requirements across all FCS apps and data regardless of the CSP used. We practice Information System Security (ISS) Incident Response (IR) for the Traffic Flow Management System (TFMS) and the Departure Spacing Program (DSP) and leverage that experience for FCS. • Our Agility Platform providing a unified interface for app and data portability, operational and development configuration management, and changes based on FAA policies and procedures. • Our price arbitrage of cloud services implemented through Agility Platform's brokering capabilities, providing an open API architecture and extensible meta model for the FAA to exploit IaaS, PaaS and SaaS requirements of existing and emerging FedRAMP service providers. CSC achieves FCS program objectives through a cost-effective cloud brokering approach, implemented in a secure hybrid cloud services model, and managed using our Agility Platform over the program lifecycle. Our hybrid cloud solution approach provides real-time monitoring, high-performance infrastructure, reliability, availability, maintainability improvements, contractor and managerial accountability, and informed programmatic decision-making resulting in cost savings and technological improvements. Our hybrid cloud solution provides for physically separated environments for NAS, Admin/Mission Support, Government Community Cloud Services, Public Cloud Services, and two physically separated co-location environments for NAS and Admin/Mission Support. CSC's cloud service integration and management approach will refine existing IT information system security (ISS) and information management. Our Agility Platform solution simplifies the challenge of monitoring and managing services across multiple cloud service providers by using a single common user interface that provides real-time control, performance, and situational awareness across all FCS environments. The Team CSC solution employs end-to-end FIPS 140-2 encryption to protect sensitive FAA information.	
Categorization of Risk:	
☐ Low Risk Data ☒ Moderate Risk Data ☐ High Risk Data	

How Contract Meets Five Essential Characteristics of a Cloud-Based Service Model:

On-Demand Self-Service: The Agility Platform provides “as-needed” infrastructure to enable required capabilities. Applications that need high availability, auto-scaling, DR/ISCP, load balancing, enhanced security, geo-redundancy, and high performance computing (HPC) can consume those services as needed. System owners and FAA management determine when (or if) applications consume services or consumption can be automated through blueprinting and the policy rules engine. CSC’s Agility Platform provides all authorized system users with self-service account management, performance monitoring, and cloud security monitoring capabilities, as well as on-demand scalability for all hosting options and tools—from storage up to monitoring. Our FCS storage solution provides for dynamic resizing of volumes (including archived volumes) with no impact to tenant applications, and allows for dynamic Input Output Processor (IOP) re-provisioning capabilities for FAA volume, obviating the need to move data. Our Agility Release Manager provides on-demand platform provisioning with embedded standard operating environments, automated application and service configuration, and management of security and operational service level agreements (SLAs) across each role in the system development life cycle (SDLC).

Broad Network Access: CSC’s hybrid cloud services capability serves as an information platform enabling data sharing across the FAA enterprise, providing access anywhere, anytime, and on any device. Our data centers and networks deliver up to 99.999 percent availability, and provide high-bandwidth, low-latency connections to public and private networks.

Resource Pooling: Hypervisors—a software layer that creates virtual machines out of pooled computing resources—provides the technical layer of our solution closest to tenant applications, virtual instances, RAM, and inter-cloud communications. Our hybrid solution incorporates three hypervisors that deliver elasticity, flexibility, and scalability to tenant applications.

- Our Biz Cloud features Microsoft’s Hyper-VR12 hypervisor to deliver virtualization management of FAA tenant applications. Hyper-VR12 natively provides elasticity of compute and memory resources. Hyper-V Network Virtualization (HNV) delivers virtualization of networking. HNV under Hyper-VR12 provides multiple approaches to network elasticity from traditional Windows Server Gateway virtualized routers to Top of Rack, load balancer, or network appliance. In our configuration for FCS, HVN incorporates F5 VIPRION load balancers to provide elasticity of network resources.
- For AWS, their Xen Hypervisor platform is Elastic Compute Cloud (EC2), which delivers compute capacity and RAM to tenant apps. EC2 Elastic IP Addresses (EIP) provides network elasticity.
- The Microsoft Azure Hypervisor delivers the virtual machine and RAM while the Fabric Controller augments elasticity, flexibility, and scalability with Caching, Access Control, and Service Bus. SQL Azure and CDN (Content Delivery) provides intra-cloud networking.

Rapid Elasticity: CSC designed our hybrid cloud ecosystem, orchestrated by the Agility Platforms, to meet the FAA’s requirements for elasticity, flexibility, and scalability over FCS’s 10-year period of performance. Powered by the unmatched scale of the commercial cloud and data center capabilities, our solution features:

- *Public Cloud:* Elasticity and flexibility of resources brokered and competed among public cloud providers. The domain is FedRAMP-compliant at a level of FISMA Moderate.
- *Community Cloud:* Elasticity and flexibility of resources brokered and competed between government community cloud providers. The domain is FedRAMP-compliant at a level of FISMA Moderate.
- *Private NAS and Private Admin/Mission Support Clouds:* Resources scaled to a planned capacity, competition limited to physically isolated domains. The domain is FedRAMP-compliant at a level of FISMA Moderate.

Non-virtual resources are physically scalable as partitions of community and private cloud infrastructure. We engineer co-located resources in excess of required capacity into our Tier III+ data centers. CSC partner EMC manages Network storage scalability and capacity through utility “pay as you go” agreements and pricing.

These capacity requirements can benefit the FAA, but the complexity can introduce risk without a comprehensive cloud management platform. Similarly, the combination of self-provisioning and the elasticity of cloud computing benefit FAA tenant applications by providing easy access to compute resources but create potential management control and governance issues with the utilization of those resources.

Measured Service: CSC’s Agility Operations module greatly simplifies FCS IT operations management functions across the heterogeneous private and public cloud environments in our solution by consolidating important monitoring, reporting, and benchmarking capabilities. Operations consolidates the technical and operational data from Team CSC’s FCS cloud providers and provides a single interface with uniform visibility into resource consumption, performance, costs, availability, and other metrics. It also provides capabilities to benchmark the performance of private and public cloud providers. NAS and Admin/Mission Support can compare cloud provider

performance across various operational parameters and limits, such as average VM provisioning time, number of failed or degraded instances, and max number of concurrent provisioning requests executed.

Cloud-Based Service Models Used In This Contract:

Cloud Services: No cloud platform has inherent value on its own without applications. On top of this hybrid cloud environment, CSC modernizes applications to bring them onto this platform and also remediates them. Additionally, we integrate SaaS and PaaS solutions onto the hybrid cloud and wrap them with full service management, monitoring, and security. CSC can extend an application’s functionality by using our Big Data and Analytics capabilities to unlock data inside them and translate it into bottom-line value. Our hybrid cloud services capability, which serves as an information platform enabling data sharing across the FAA enterprise, amplifies bottom-line value.

Infrastructure as a Service (IaaS): CSC’s Agility Platform provides the infrastructure and models the Plan-Build-Consume-Run cycle of analyzing, building, consuming, and deploying FAA cloud resources. Each module interacts to plan existing and new application FCS deployments, building stacks, packaging applications, and interactive scripts available to the FAA IT consumers for consuming and running IT assets in the FCS. These features are automated. The Agility Platform wraps this into a policy-driven and secure framework. Within this, different communities of FAA IT users will interact with the four major workspace models (Agility Designer, Agility Store, Agility Operations, and Agility Release Manager), each providing unique capabilities to specific roles across the application lifecycle.

Platform as a Service (PaaS): CSC’s Agility Designer module enables FAA system owners to rapidly assemble everything from simple stacks to highly complex multi-tier application blueprints and topologies, and enables these workloads to have the cloud portability that FAA needs to avoid vendor lock-in. Agility Platform’s graphical design environment accelerates FAA’s design and assembly process of complex application blueprints containing cloud portable workloads with a user-friendly point-and-click interface. Using Designer, we assemble NAS and Admin/Mission Support workloads such as development platforms, custom business applications, and packaged applications into blueprints and outfitted with application configuration controls, auto-scaling rules, storage tiers, security settings, governance controls, and embedded with operating environment agents and utilities. To accelerate design and assembly for the FAA, Designer includes a version-controlled library for reusable standard operating environments and deployment accelerators including customizable templates, scripts, blueprints, policies, packages, and more. Designer allows FAA developers and architects to construct a versatile “everything as a service” portfolio that is policy-compliant and remains portable across heterogeneous cloud types. When these cloud workloads are assembled, they can be seamlessly promoted to the next lifecycle stage for publishing and end user consumption. CSC’s Agility Store provides a fully governed, self-service portal to enable an “everything as a service” portfolio of business applications, development platforms, and third-party SaaS, PaaS and IaaS. Agility Store provides an intuitive interface to support users ranging from developers needing development platforms, to nontechnical users accessing third-party SaaS offerings, mobile applications, and desktop resources. The initial scope of the FCS focuses on IaaS and co-location, but Team CSC collaborates with NAS and Admin/Mission support to identify additional services to meet evolving FAA requirements. Store users can conduct detailed searches for IT resources, and customize and republish assets where appropriate and allowed by FAA policy. When offering self-service capabilities in Agility Store, FAA can collect user feedback, reviews, and ratings to provide quality control for service portfolio optimization. Agility Store tracks resource consumption including customizable charge-back and cost center assignment features. All Store resources and assets also remain accessible via Agility Platform’s governance-enforced API.

Software as a Service (SaaS): CSC’s Agility Release Manager module allows for customization of FAA software lifecycle stages to reflect each group’s SDLC and establishes role-based permissions to promote, accept and approve software builds. With Release Manager, the FAA can leverage policies and enable release automation across stages, or introduce manual release approval processes with integration into FAA’s existing SDLC tool chains and approval workflows. Agility Release Manager accelerates broader FAA initiatives for DevOps, continuous delivery, and integration. Its capabilities and benefits include on-demand platform provisioning with embedded standard operating environments, automated application and service configuration, and management of security and operational SLAs across each role in the SDLC. Agility Release Manager leverages these high-fidelity, production-like, run-time environments across the lifecycle and achieves cycle time reductions while preventing the introduction of configuration errors and other defects downstream into production environments.

Monitoring as a Service (MaaS): Team CSC provides a scalable Monitoring as a Service Solution (MaaS) using the Agility Platform Monitor and Nimsoft. The Agility Platform Monitor provides tenant applications with a

common Application Programming Interface (API) that fully supports Simple Network Management Protocol (SNMP) and allows implementation of Management Information Base (MIB) files to obtain real-time status of FCS service use. Nimsoft offers a comprehensive set of capabilities supporting MaaS including the ability to:

- Rapidly create and enable custom SNMP-based monitoring for servers, storage, and network devices.
- Configure unique polling requirements per MIB object, as defined by the tenant application owner.
- Support dynamic SNMP tables with flexible indexing.
- Browse MIBs to rapidly manage the variables on any SNMP-compliant device.
- Support SLA monitoring and reporting on any polled MIB.

Nimsoft modules address the MaaS requirements. The SNMP Gateway easily integrates with other network and server management solutions and transforms CA Nimsoft alarm messages to SNMP trap messages that any SNMP-based event manager can read. The Agility Platform Monitor provides the tools for tenant application developers to access Nimsoft capabilities, define and control MaaS functions inside Agility blueprints created for each application, and group performance attributes into logical views that can be accessed programmatically and through the Performance Management User Interface.

Deployment Method:

☐ Private Cloud ☐ Community Cloud ☐ Public Cloud ☒ Hybrid Cloud

Accomplishments/Customer Feedback:

We implement our brokered cloud service solution through a hybrid cloud architecture and control it through our price management mechanism and Agility Platform tool. Our brokered cloud service manages CSP costs and services to ensure FAA has the best cloud service at the best price.

4.2.3 Federal Aviation Administration (FAA) Enterprise Messaging System (EMS) [CSC Contract]

Agency:	Federal Aviation Administration (FAA)
Contract Full Name:	Enterprise Messaging System (EMS)
Contract Short Name:	FAA EMS
Contract Number:	DTFAWA-12-D-00021
Contract Type:	Indefinite Delivery Indefinite Quantity (IDIQ)
Period of Performance:	05/21/2012 to 05/20/2019
Total Contract Value:	\$92,306,692

Overview/Scope of Work:

The scope of this contract includes a cloud messaging service for the FAA and potentially other Department of Transportation (DOT) organizations, including all the required features, functions, and services related to transition, implementation, and operation. The FAA's prior messaging system, a client-server based solution, used the IBM Lotus Notes and Lotus Domino product lines. Other DOT organizations used Microsoft Exchange. The agency determined that the traditional client-server approach to its current messaging system did not meet the need to access any data, anywhere, anytime, using any device, in the most cost-effective way. CSC helped the FAA with the agency's first entry into the cloud by transitioning it to a seamless enterprise wide, commercially available cloud messaging service for approximately 80,000 users in DOT's Headquarters and agencies located in each of the 50 states, the District of Columbia, Puerto Rico, and some international locations. CSC carried out a phased approach to the FAA's first entry point into the cloud to assure a smooth transition from the current infrastructure environment to cloud services.

CSC's solution for the EMS addresses the requirements and objectives of the contract, based on Office 365 D-ITAR (International Traffic in Arms Regulations), a commercially proven cloud messaging system (CMS). The solution also encompasses FAA's facilities; IT equipment and infrastructure; current support systems and product configurations; software licensing and any necessary third-party licensing; specialized product configurations; and any facilities, networks, Internet access, support services, and the related communications infrastructure necessary to deliver and sustain the CMS.

CSC's solution meets all specified security requirements and implements safeguards to protect confidentiality,

integrity, and availability in all aspects of the cloud messaging service during implementation and service delivery. CSC complies with the requirements of the FISMA and NIST standards for Moderate Impact systems (as defined by NIST Federal Information Processing Standard (FIPS) 199 and NIST SP 800-53 Rev 3). CSC supplies the FAA's Cyber Security Management Center (CSMC) or the US Computer Emergency Readiness Team (US-CERT) with access to security logs and other incident information in accordance with US-CERT reporting requirements specified in the US-CERT Federal Incident Reporting Guidelines to investigate potential security events. CSC, through our CSP team member, Complies with International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2005 and 27002:2005. CSC and its CSP comply with all FedRAMP requirements for the acquisition of cloud services.

Categorization of Risk:

☐ Low Risk Data ☒ Moderate Risk Data ☐ High Risk Data

How Contract Meets Five Essential Characteristics of a Cloud Based Service Model:

On-Demand Self-Service: FAA's email administrators can unilaterally provision new email user accounts without the assistance of CSC or Microsoft and can adjust their storage needs as required. The solution also provides administrators with the tools to assign ownership rights to another user's mailbox, such as accessing dormant accounts. Our solution also provides an on-demand email archiving solution that addresses three key challenges: email storage management, legal discovery, and regulatory compliance. The FAA/DOT can unilaterally provision these capabilities without contractor or provider assistance. The users can also change and reset their own passwords.

Broad Network Access: The seven-year effort includes 18 FTEs and provides support to 60,000 FAA users and 20,000 other DOT users at DOT headquarters and agencies located in each of the 50 states, District of Columbia, Puerto Rico, and some international locations. CSC supports 60,000 desktop/laptop users, 20,000 Internet access-only users, and 30,000 mobile devices.

Resource Pooling: The service is designed as a multi-tenant model where various FAA and DOT departments share the same system. The solution also supports sharing and delegation of address lists, mailboxes, and calendars through Exchange ActiveSync.

Rapid Elasticity: CSC based our solution on Office 365 D-ITAR, bringing together cloud-based versions of Microsoft's communications and collaboration products with the latest version of the Microsoft desktop suite. This solution can migrate 80,000 user accounts, and has the flexibility to expand or contract the number of user accounts on demand.

Measured Service: The solution provides 25GB mailbox size per user, with the ability to send messages up to 50MB, including attachments. The FAA has the ability to change the email size and control attachment size. Users can send emails to an unlimited number of recipients per day—a feature that exceeds the FAA's previous limit of 500 unique recipients a day. The system has multiple types of storage limit notifications based on size. Exchange Online provides a **Warning** when the user's mailbox approaches maximum size, a **Prohibit Send** notification when the mailbox reaches its size limit, and a **Prohibit Send/Receive** notification when the mailbox reaches its size limit and the system sends the user a non-delivery report (NDR). The user cannot receive new messages until he or she deletes enough email and cannot send out messages either, but can save them to send after the mailbox size falls below the limit.

Cloud Based Service Model(s) Used In This Contract:

Email as a Service (EaaS): The FAA requires a cloud messaging service that incorporates leading technology and commercial best practices while meeting the statutory and regulatory requirements inherent to the FAA's mission. The FAA service is Dedicated Microsoft Office 365 D-ITAR, which requires more capacity planning and higher security features than Government Community Cloud. FAA EMS tasks include Project Planning and Control; Discovery and Migration Services; EaaS; and EaaS Implementation. CSC's work under this contract supports the FAA's efforts to transition from legacy client-server based messaging solutions to a Section 508-compliant CMS that allows access to data anywhere and anytime through a full spectrum of devices. The solution must also comply with all applicable laws and Federal regulations regarding security and privacy safeguards, including the Federal Information Security Management Act (FISMA), Privacy Act, relevant OMB guidance, FAA regulations and policies, and other relevant mandates, such as the Freedom of Information Act (FOIA) and the electronic discovery (eDiscovery) requirements of the Federal Rules of Civil Procedure.

Software as a Service (SaaS): CSC's Office 365 D-ITAR solution comprises a suite of productivity applications,

which includes the following products delivered as SaaS:

Microsoft Exchange Online. Provides a full set of features and functions for email, calendar, and contacts from anywhere and at any time, on desktops, laptops, and mobile devices.

Microsoft SharePoint Online. Provides SharePoint Online, which allows the FAA to collaborate and share information with anyone, anywhere. The solution provides a flexible, Web-based suite of tools and services to help employees manage information and effectively collaborate across the organization. CSC supports the customization and hosting of applications. SharePoint Online also includes other features, such as business intelligence and business process forms.

Microsoft Lync Online. Provides cloud-based instant message, presence, and online meeting experiences.

Microsoft Office Web Apps. Provides Office Web Apps as the online companion to Microsoft Word, Excel, PowerPoint, and OneNote.

Proofpoint Archive. Provides an on-demand email archiving solution that addresses three key challenges: email storage management, legal discovery, and regulatory compliance. Appropriate members of Team CSC will address these challenges and the methods to tackle them in jointly held meetings.

Deployment Method:

☒ Private Cloud ☐ Community Cloud ☐ Public Cloud ☐ Hybrid Cloud

Accomplishments/Customer Feedback:

Task 3 – Email as a Service

- Provided EMS solution built on Microsoft Office 365; brings together cloud based versions of Microsoft’s communications and collaboration products including Microsoft Exchange Online, Microsoft Lync Online, Microsoft Office Web Apps, SharePoint Online and Proofpoint Archive.
- Supported EaaS solution using SLAs, including monthly uptime (< 95%), scheduled downtime, and unscheduled downtime.

Task 4 – EaaS Implementation

- Set up configured EaaS capabilities and services.
- Provided detailed plans including kick-off sessions, training, and daily communications to help educate users about rationale for changeover to the CMS system, and orient users to new cloud-based environment.
- Created core SOPs that became basis for live help desk, systems administration and operations training; delivered to multiple operating divisions, each with its own legacy procedures, support staff and service providers.
- Developed, delivered self-paced, web-based and video end-user training, and brown bag training sessions based on user feedback. Planning ensured all training sessions, materials delivered on time before migration.
- Migrated functionalities, custom and modified solutions.
- Provided Tier 3 help desk services, technical support. Tier 3 help desk responds to service requests from the FAA Tier 2 Help Desk; handled 173 service requests during first six months of contract, including 14 Severity Level 1 SRs which we responded to IAW SLAs.

Customer Feedback

“During a delivery assurance review by an independent unit of CSC, the reviewers heard from the customer that the CSC fielded a “highly motivated, mission focused team.”

“CSC team and client have established strong working relationship.”

“Joint CSC team and client capture of Lessons Learned on a quarterly basis is a best practice.”

4.2.4 Department of Justice (DOJ) Drug Enforcement Administration (DEA) Firebird Infrastructure Technology Services (FITS) II [SRA Contract]

Agency:	Department of Justice (DOJ) Drug Enforcement Administration (DEA)
Contract Full Name:	Firebird Infrastructure Technology Services (FITS) II
Contract Short Name:	DEA FITS II
Contract Number:	GS00Q09BGD0055 / DJD-11-HQ-E-0045
Contract Type:	Firm Fixed Price (FFP)
Period of Performance:	06/01/2011 to 05/31/2021
Total Contract Value:	\$74,900,000
Overview/Scope of Work:	
FITS II encompasses the software development life cycle (SDLC) process, and SRA incorporates the areas of Cloud Computing, Private Cloud Virtualization, Platform as a Service (PaaS), Lab as a Service (LaaS), and Development/Test as a Service (DTaaS) into a single environment called Lab 2.0 as part of its SDLC solution profile. FITS II exemplifies SRA's experience with enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources that we can rapidly provision and release with minimal management effort or service provider interaction. SRA has supported DEA's Firebird IT infrastructure since 2004. Based on our successful performance on the 2004-2009 FITS I contract, DEA awarded SRA the 10-year, \$72.9M FITS II contract for providing enterprise-wide engineering services to sustain and modernize the worldwide IT infrastructure supporting more than 16,000 users at 226 US sites and 85 sites in 66 other countries. We engineer and sustain LANs, WANs, servers, storage, communications services, security, desktops, laptops, and mobile devices. The FITS II contract provides system, server, and workstation integration services to the DEA Information Systems organization. In addition to the team's integration duties, the FITS II team performs all field office installations, migrations, and technical refreshes, and provides continuous build/patch support for DEA's 17,000+ workstations and servers worldwide.	
Categorization of Risk:	
☒ Low Risk Data ☐ Moderate Risk Data ☐ High Risk Data	
How Contract Meets Five Essential Characteristics of a Cloud Based Service Model:	
On-Demand Self-Service: SRA built its Lab 2.0 environment so all legacy development and infrastructure integration projects can take place in a virtual private cloud environment that mimics the Firebird production environment. SRA built self-service features into Lab 2.0 to facilitate users' access and control of their labs. Broad Network Access: SRA developed Firebird Anywhere (FBA), which enables users to securely access DEA's sensitive but unclassified network using their personal computing device. SRA has architected and implemented an enterprise-class Virtual Desktop Infrastructure (VDI) solution, which provides the complete desktop experience on any computer or iOS/Android mobile device that meets minimum security requirements and enables users to seamlessly switch between devices while maintaining their current sessions. Our VDI implementation has enabled DEA's employees and contractors to effectively telework while increasing the overall security posture. SRA implemented the Mobile Device Management platform (using Airwatch), which allows DEA to manage and secure all of the mobile devices the DEA staff uses. Resource Pooling: SRA developed the Lab 2.0 environment for the DEA as a PaaS and currently works with other DOJ components to offer them access for project and software development. Rapid Elasticity: The DEA VDI environment can scale for demand. There are policies in place to provision additional virtual desktops when certain thresholds are exceeded, and when demand subsides, those desktops can be shut down. Measured Service: SRA or other client administrators can monitor an entire environment from the Citrix Director console. This console serves as a dashboard for the performance of the environment where we can monitor bandwidth, server activity, and desktop pool capacity. We can also look at the performance of a single desktop session. The network operations center (NOC) can use this tool for real-time performance monitoring.	

Cloud Based Service Model(s) Used In This Contract:

Platform as a Service (PaaS): SRA offers PaaS to the DEA as part of SRA's Lab 2.0 environment, which incorporates PaaS, DTaaS, and LaaS into a single system. Lab 2.0 provides any DEA organization with the ability to use a working copy of Firebird to test software or new products before deploying to production. The systems engineering, operations, and development groups primarily use PaaS. Other DOJ components have asked to use the Lab 2.0 environment for their development projects and we work to provide them access. We can provide a service catalog of items, such as standard OS images with current Defense Information Systems Agency (DISA) Security Technology Information Guidelines (STIGs) applied.

Lab as a Service (Laas): SRA provides full lifecycle engineering support to the Firebird enterprise network, including its infrastructure systems. We engineered, implemented, and provided advanced engineering support for systems such as: Symantec SEE, BigFix in our labs, MS SCOM 2012, and MS SCCM 2012. We engineered DEA's VDI environment using VMware/Citrix and support DEA's LaaS for application development, software testing, and testing new hardware. We engineered the upgrade of DEA's VM environment for application hosting. We stood up SharePoint 2010 and Project Server 2010, which we use to manage Firebird IT projects.

Development/Test as a Service (DTaaS): SRA uses a virtualized private cloud environment for software development, engineering, integration, testing, and troubleshooting. We provide development and test environments for the software development teams and provide troubleshooting assistance to developers. We consolidated labs into a central private cloud model (Lab 2.0). We used VMware vCenter 5.5 WebClient to provide virtual environments that mirror production servers. We use self-service features to facilitate users' access and control of their labs. All legacy development and infrastructure integration projects occur in a virtual private cloud environment that mimics the Firebird production environment. We built the Lab 2.0 environment using HP Blade and Dell R900 Series servers using VMware's vCloud, vSphere5.5 WebClient. We reduced the time to create development and test environments by 90% — from five days to four hours. We provide mirror images of the Firebird infrastructure for designing, developing, and testing new capabilities in a Firebird replica before putting them on the enterprise network. We maintain test beds for evaluating application changes segmented from production operations to enable the development groups and DEA QA to validate application readiness before deploying.

Low Risk Data and Cyber Security: SRA implements government-mandated security controls in all solutions we design and deliver. We implement Secure Technical Implementation Guides (STIGs) for all servers, workstations, and network components in the production environment. We incorporate Data-at-rest and Data-in-transit security requirements. We provide documentation and support for independent security risk assessments and certification and accreditation requirements. SRA developed and implemented a Homeland Security Presidential Directive-12 solution that meets OMB and DOJ requirements for access to DEA's Firebird environment. This initiative implements two-factor authentication, single sign-on, and digital signature. SRA worked with engineers from the DOJ Identity Management office to set up PIV Card authentication on Firebird in accordance with DOJ guidance.

Deployment Method:

☒ Private Cloud ☐ Community Cloud ☐ Public Cloud ☐ Hybrid Cloud

Accomplishments/Customer Feedback:

Accomplishments on this contract that involve cloud computing include:

- SRA reduced the time to create development and test environments by 90% — from 5 days to 4 hours.
- SRA completed all requirements on time, cutting their time to delivery capability to three-to-six months per project.
- SRA managed financial performance within an average variance of 3%.
- In the June 2011-May 2012 Contractor Performance Assessment Reporting System (CPARS) evaluation of SRA's FITS support, DEA stated: "Both Formal and Working deliverable products have been first rate. The quality of integration services has been very good. SRA successfully executed all of its contract requirements on schedule for this period and consequently DEA was able to begin and complete specific projects on time. SRA has been extremely flexible in aligning their staff (both key and others) with the government's requirements. [SRA] has exhibited excellent business relations with all customers. [SRA] has exhibited very good management of key personnel. [SRA] has been able to attract and retain qualified personnel."
- "Given what I know today about [SRA's] ability to execute what they proposed in their proposal, I definitely would award to them today." — *Procurement Analyst Amanda Marsh*

4.2.5 Department of Health and Human Services (HHS) Health Resources and Services Administration (HRSA) National Practitioner Data Bank (NPDB) [SRA Contract]

Agency:	Department of Health and Human Services (HHS) Health Resources and Services Administration (HRSA)
Contract Full Name:	National Practitioner Data Bank (NPDB)
Contract Short Name:	HRSA NPDB
Contract Number:	HHSN316201200050W
Contract Type:	FFP and T&M with performance metrics
Period of Performance:	6/21/2012 to 06/30/2017
Total Contract Value:	\$70,080,597
Overview/Scope of Work:	
For 21 years, SRA has served as a trusted partner on the National Practitioner Data Bank (NPDB) program, a national clearinghouse to collect and release information related to the professional competence and conduct of health care practitioners. We deliver full IT systems, business intelligence, data integration and warehousing, security services, customer service operations, and continuous improvement of NPDB services and capabilities. We designed, developed, engineered, and implemented the system, and assume responsibility for maintenance, operations, and system enhancements. In November 2014, we reengineered NPDB hardware, software, and communications systems to incorporate the AWS's Web-based and cloud computing technology. HRSA exemplifies SRA's experience with enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that we can rapidly provision and release with minimal management effort or service provider interaction. NPDB processes more than 5.5 million transactions per year for more than 150,000 registered users at 19,500 registered health care organizations nationwide. It contains more than 1.2 million adverse action reports on over 625,000 health care practitioners annually, and receives approximately 1,000 new reports each month. NPDB generates over \$20 million annually for the government through its online fee-for-service e-commerce model. Under the current \$70M, five-year NPDB contract, SRA provides full software and systems lifecycle support, including program management; enterprise customer relationship management; leasing of hardware and software (HW/SW), IT acquisition, HW/SW maintenance, database administration, and implementation of standards; operations and maintenance (O&M); business analytics and data integrity; security services, functional and performance testing, and research and marketing support.	
Categorization of Risk:	
☐ Low Risk Data ☒ Moderate Risk Data ☐ High Risk Data	
How Contract Meets Five Essential Characteristics of a Cloud Based Service Model:	
On-Demand Self-Service: SRA can modify instance sizes supporting the NPDB on-demand based on AWS's CloudWatch metrics, Splunk alerts, and custom monitoring scripts. SRA can create full environments on demand, and created training environments to support HRSA and NPDB user demands. Broad Network Access: The Web-based NPDB interface remains available on all platforms, including workstations, laptops, and mobile devices. SRA develops all Web applications using a framework that renders on mobile devices and mobile platforms. Approximately 15% of the health care practitioners that query the NPDB today now use a mobile device. Resource Pooling: Health care entities use NPDB, such as hospitals, managed care organizations, and medical practitioners, and individual subscribers. NPDB leverages the AWS Elastic Compute Cloud (EC2) and Relational Database Service (RDS) native resource pooling. Rapid Elasticity: The AWS EC2 service comes with an Auto Scaling feature that helps maintain application availability and allows HRSA to scale capacity up or down automatically according to defined conditions. Auto scaling helps ensure that enough Amazon EC2 instances run at any given time, and it can also automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance, and decrease capacity during lulls to reduce costs. Auto Scaling proves suited for applications that have stable demand patterns or experience hourly, daily, or weekly usage variability. SRA develops and regularly updates cloud capacity plans and planning strategies to ensure user availability at all times. Measured Service: NPDB can leverage AWS CloudWatch's metrics and scale and optimize resources, such as	

instance size and number of virtual instances. We track these resources via the AWS Management Console. SRA also manages all NPDB fees and other HHS financial transaction processing in compliance with federal and HHS governance. We use the AWS EC2 system to produce weekly and monthly financial reports detailing the money collected daily classified by credit card, electronic funds transfer (EFT), credit card charge back, and EFT returns. We also produce a semiannual report with uncollectable charges that goes to the customer's Division of Financial Operations for collection.

Cloud Based Service Model(s) Used In This Contract:

Infrastructure as a Service (IaaS): HRSA wanted to reduce operational costs related to hardware, software, hosting, and other associated costs. SRA analyzed cloud delivery and service models and determined that an IaaS solution would be the more cost-effective and less disruptive option, considering the need to minimize change and build redundancy into the current Oracle solution and take security and cost into consideration. Based on technical capability, cost, and security, HRSA selected the AWS Elastic Compute Cloud (EC2) environment. We designed the NPDB system architecture, evaluated our proof-of-concept prototype with the customer, and successfully completed the migration in six months. We moved the full NPDB system to the virtual AWS EC2 cloud environment in November 2014. We achieved an authority to operate using the AWS EC2 environment.

Software as a Service (SaaS): SRA has evolved the NPDB into a seamless, role-based system that provides easy, secure access to authorized data through a common interface. We developed SaaS Web applications that provide query, reporting, and matching mechanisms on adverse actions reports. These are event-based—when users submit new reports, NPDB automatically matches them against continuous queries, and the system forwards the results to entities in near real time. SRA develops all Web applications using a framework that renders on mobile devices. Approximately 15% of the health care practitioners who query the NPDB today now use a mobile device. We provide operational support, software maintenance, and upgrades to the NPDB cloud architecture to ensure the fastest possible turnaround for the automated workflows. We perform software installation, configuration, and upgrades in our AWS EC2 environments. SRA has achieved system availability/accessibility of over 99.98 percent over the past two years.

Deployment Method:

☐ Private Cloud ☐ Community Cloud ☒ Public Cloud ☐ Hybrid Cloud

Accomplishments/Customer Feedback:

SRA delivered all generations of the NPDB system on schedule and within budget. Since migrating the NPDB application and data to AWS, SRA has helped HSRA reduce its system operating costs by \$80,000 per month, while boosting self-service activity by streamlining credit purchasing processes and fees.

SRA has produced 100% of deliverables on time. We employ a five-year integrated master project schedule to identify all planned software releases and other deliverables, and have encountered no problems delivering hardware and software.

SRA has had no cost overruns. Through self-query fees, SRA's NPDB program contributes about \$20M annually to federal revenue.

- SRA manages all project schedules, milestones, and deliverables associated with the NPDB system. HRSA rates SRA against 23 performance metrics. The performance metrics cover system availability, system responsiveness, customer service center performance, operational performance, and subject customer satisfaction metrics. HRSA has rated SRA outstanding on 95% of all performance metrics over the last 10 years.
- SRA has scored "outstanding" in performance-based metrics such as system availability, system responsiveness, customer service center performance, operational performance, and customer satisfaction while operating in a fixed-price environment. As evidence of our success, HRSA awarded SRA the current contract to continue support through 2017.
- "Given what I know today about the contractor's ability to execute what he promised in his proposal, I DEFINITELY WOULD award to him today given that I had a choice." — *Contracting Officer Donnie O'Brien (2012 CPARS)*

4.3 FINANCIALS (D&B NUMBER) [6.3]

On November 27, 2015, CSRA Inc. (CSRA) became an independent company through the spin-off by CSC of its US public sector business, CSGov. On November 30, 2015, CSRA completed its combination with SRA International, Inc. and began trading on the New York Stock Exchange as a public company.

CSRA Inc. is a financially strong and responsible provider of enterprise IT and cloud services to US state and federal government customers.

Because CSGov (DUNS #079735371) operated as a subsidiary of another company, SRA (DUNS #097779698) operated as private, and CSRA (DUNS #080011988) has only traded publicly for three months, Dun & Bradstreet (D&B) does not have the accurate nor complete information to provide a defensible credit rating. D&B said paying for its research services would not yield a valid rating in time for proposal submission. If required, CSRA would certify to appropriate D&B status after award. Still, recognized sources demonstrate CSRA's financial strength and stability. **Exhibit 4-3** shows CSRA's most recent balance sheet.

The D&B Credit Rating measures a firm's size and composite credit appraisal, based upon information from a company's interim or fiscal balance sheet and an overall evaluation of the firm's creditworthiness. The requirement for a 3A2 rating breaks down as follows:

- **3A:** company worth between \$1 million and \$10 million.
- **2:** Composite Credit Appraisal of "2" on a scale from "1" through "4," reflecting D&B's overall assessment of a firm's creditworthiness based on D&B's analysis of company payments, financial information, public records, business age and other important factors. A "2" is the highest Composite Credit Appraisal possible for a company that does not supply D&B with current financial information.

Company Worth. The bidding entity, CSC State and Local Solutions, LLC, a wholly owned subsidiary of CSGov and subsequently CSRA, does not file separate financial statements. As of January 1, 2016, CSRA had \$204 million in cash and cash equivalents on its balance sheet, \$1.1 billion in current assets, and \$3.4 billion in total assets. In addition, based on the stock price as of February 16, 2016, the enterprise value of CSRA is \$7.0 billion. The firm exceeds the size standard.

Credit Appraisal. Parts of the organization have received D&B ratings consistent with the required credit appraisal score. For example, our PayDex scores typically in the 70s and our viability score of "2" indicates a low risk of going out of business in the next 12 months. Moreover, CSRA has \$500 million available on its credit revolver and generates a free cash flow roughly three times its debt service. The three major credit rating agencies performed a more complete assessment of CSRA's credit last fall, when the company raised debt to accomplish the spin-out and merger. Upon completion of the merger, Fitch reaffirmed its investment grade rating of "BBB-." CSRA's interest payment on its debt is less than 3%, indicating that the market views CSRA as very low credit risk.

CSRA INC. COMBINED CONDENSED BALANCE SHEETS (unaudited)		
(Dollars in thousands)	As of	
	January 1, 2016	April 3, 2015
Current assets		
Cash and cash equivalents	\$ 204,469	\$ 4,979
Receivables, net of allowance for doubtful accounts of \$20,429 (fiscal 2016) and \$14,733 (fiscal 2015)	740,511	696,727
Prepaid expenses and other current assets	133,023	92,665
Total current assets	1,078,003	794,371
Intangible and other assets		
Goodwill	2,344,457	802,582
Customer-related and other intangible assets, net of accumulated amortization of \$167,221 (fiscal 2016) and \$150,295 (fiscal 2015)	902,799	33,405
Software, net of accumulated amortization of \$93,030 (fiscal 2016) and \$75,544 (fiscal 2015)	38,769	35,261
Other assets	72,275	58,931
Total intangible and other assets	3,358,300	930,179
Property and equipment, net of accumulated depreciation of \$792,539 (fiscal 2016) and \$696,796 (fiscal 2015)	501,174	436,732
Total assets	\$ 4,937,477	\$ 2,161,282
Current liabilities		
Accounts payable	\$ 144,124	\$ 130,551
Accrued payroll and related costs	217,703	109,539
Accrued expenses and other current liabilities	468,522	440,606
Current capital lease liability	27,871	21,351
Current maturities of long-term debt	80,000	—
Dividends payable	16,252	—
Total current liabilities	954,472	702,047
Long-term debt, net of current maturities	2,871,906	—
Noncurrent capital lease liability	111,928	129,933
Noncurrent deferred income tax liabilities	194,931	153,297
Other long-term liabilities	576,008	80,957
Commitments and contingent liabilities		
Equity		
Net Parent investment, prior to Spin-Off	—	1,067,492
CSRA Stockholders' Equity:		
Common stock, \$0.001 par value, 750,000,000 shares authorized, 162,621,486 shares issued and outstanding	162	—
Additional paid-in capital	160,946	—
Earnings retained for use in business	15,215	—
Accumulated other comprehensive income (loss)	29,877	(405)
Total CSRA stockholders' equity	206,200	1,067,087
Noncontrolling interests	22,032	27,961
Total equity	228,232	1,095,048
Total liabilities and equity	\$ 4,937,477	\$ 2,161,282

Exhibit 4-3. CSRA Balance Sheet. SRA and CSGov combined to form CSRA, a financially stable large systems integrator.

4.4 GENERAL INFORMATION [6.4]

4.4.1 Depth and Breadth of Services in the Cloud Marketplace [6.4.1]

For more than 12 years, CSRA has helped our government clients' journey to the cloud. Together, we have taken steps such as virtualizing data centers all the way to full cloud broker services as depicted in **Exhibit 4-4**. In doing so, we have built up expertise in cloud offerings. CSRA offers our clients solutions and services for SaaS, IaaS, and PaaS.

CSRA is a systems integrator and cloud broker. This allows us to provide a depth and breadth of services that no single cloud service provider can match. We provide all the services available from the leading cloud providers in the marketplace, AWS and Azure, through a single user interface. We can also provide additional services such as fully dedicated private clouds that larger cloud service providers may not offer the customer. Through evaluating cloud solutions for the best solutions, and through solution

development sessions with our alliance partners, we provide IaaS, PaaS, and SaaS from the market's best vendors. CSRA tests new capabilities added to the public market for client applicability and ease of migration to and from the service so they meet security regulations before we bring them to our customers. As a result, Participating Entities are not locked into any one service and those services meet the security and privacy requirements. On customer request, we can increase the priority of adding a commercial solution to our catalog. We also provide migration services, cloud managed services (e.g. help desk, patch management), governance, and consultancy services (design and architecture, certification and accreditation support). This allows entities to get the full service they need without having to go to multiple service providers. CSRA has deployed this same model with the state of California and the Federal Aviation Administration.

The CSRA solution contains services for every service model and data risk level combination that Participating Entities requires. We offer IaaS from the leaders in commercial market, AWS and Azure. CSRA also offers ARC-P, a FedRAMP accredited IaaS system that we can place in the customer's data center for additional security.

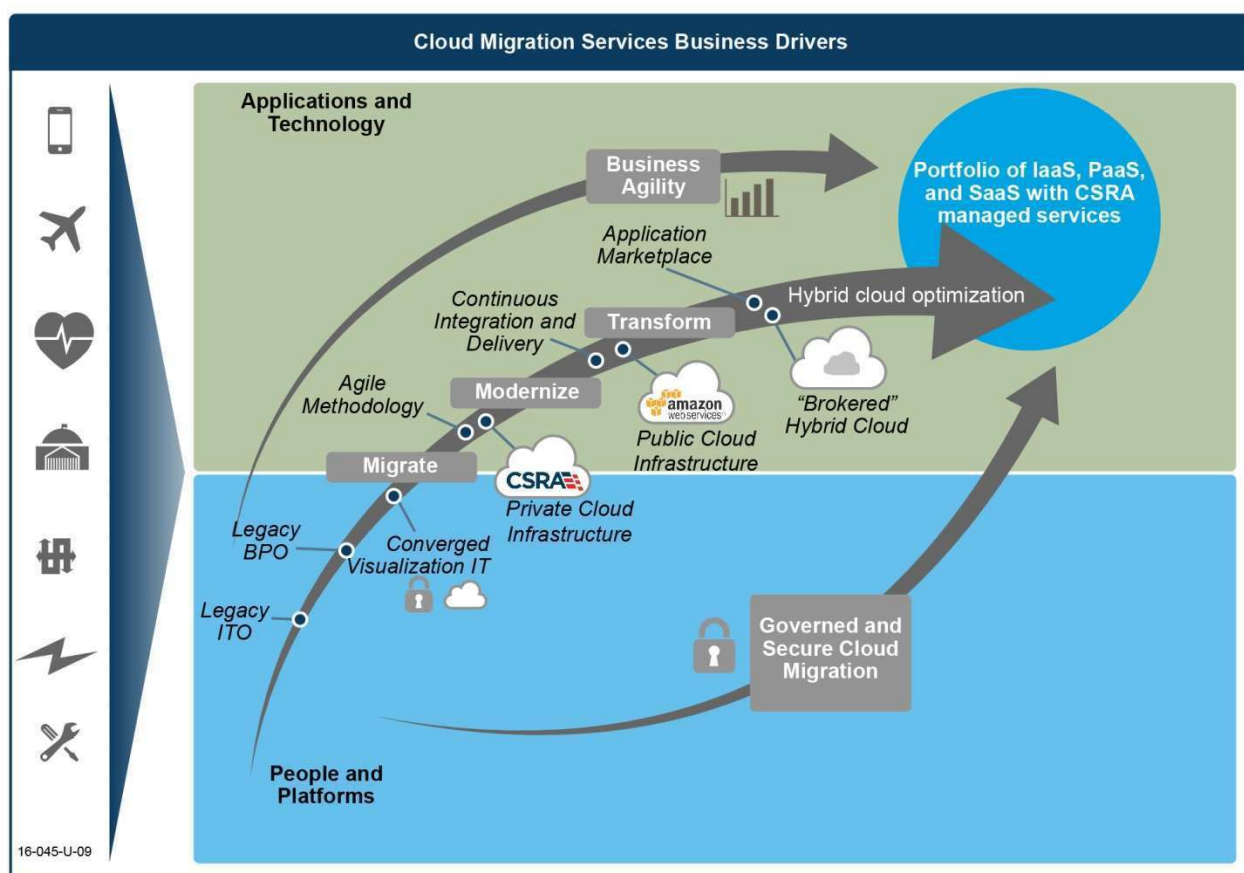


Exhibit 4-4. Cloud Migration Services. CSRA has helped more than 10 government clients in their migration to the cloud.

We have development PaaS solutions (AppWorks & ARCWRX), CRM SaaS (Microsoft Dynamic), and ITSM SaaS (ServiceNow). CSRA also offers leading collaboration and office productivity SaaS with Office 365 and Skype for Business in our solution.

All of these are just the initial offerings. Throughout the 10-year term of this MSA, CSRA will add more services to meet the evolving needs of Participating Entities.

4.4.2 Auditing Capabilities and Reports [6.4.2]

All of CSRA's vendors', Microsoft, Amazon, and ServiceNow, auditing capabilities and reports are consistent with SAS 70 or later. CSRA's ARC-P and ARCWRX are FedRAMP compliant which has equally strict auditing capabilities and reports requirements.

4.5 BILLING AND PRICING PRACTICES [6.5]

CSRA commits to participation in the Federal Communication Commission's E-rate discount program without the addition of any service or contract fee. Our E-Rate team understands the process of seeking E-Rate funding. Because funding depends on compliance, we support and facilitate compliance. Our experience working with organizations to seek E-Rate funding spans the years of the E-Rate program. CSRA uses the service provider identification number 143024093 listed on the USAC website under "Computer Sciences Corporation."

4.5.1 Billing and Pricing Practices [6.5.1]

CSRA's Cash Operations (CO) generates invoices based on costs incurred and recorded in our Costpoint accounting system. Internal control and monitoring of the billing process also includes maintaining accessible lines of communication with departments such as Compliance, Contracts, Project Accounting, General Ledger, and the Program Control Office (PCO). Due to the complexity and variety of contracts within CSRA, the procedures vary by customer and contract. Specific instructions are contained in our Customer Contract files to support consistent, compliant, transparent, and easy to understand billing practices.

CSRA uses an estimating system to support the development of consistent and accurate price estimates in accordance with all government (federal, state, and local) regulations and guidelines, CSRA policies, procedures, and disclosed accounting practices. CSRA develops all cost/price estimates in full compliance with the CSRA estimating system.

For each addendum to the contract, CSRA will propose a set of milestones for payment that we will negotiate with the Purchasing Entity. Our bills for the addendum will include the milestones completed and accepted for the period when we prepared the bill. If the addendum includes T&M labor content, we will identify CSRA employees and show hours they worked, and we will also include the hourly rate to calculate the amount billed for the period the bill covers.

4.5.2 Typical Cost Impacts Implementing the Solution [6.5.2]

The services to be supplied are on a firm fixed-price basis. Cost impacts will likely only occur if a Purchasing Entity requests additional work outside the scope of the delivery or work in addition to the scope that has been agreed to. For instance, if the scope of the Addendum requires 500 users for the system delivered and the Purchasing Entity finds that they need to have 1,000 users, there may be a cost impact in order to double the required users.

4.5.3 NIST Compliance [6.5.3]

CSRA's solutions are fully compliant with NIST, as defined in NIST Special Publication 800-145, for the IaaS, PaaS, and SaaS. These solutions meet the essential characteristics for cloud computing. They are provided on-demand and with self-service, broad network access, resource pooling, rapid elasticity and as a measured service. We go into further detail in Section 6.1.2.

4.6 SCOPE AND VARIETY OF CLOUD SOLUTIONS [6.6]

As a systems integrator, CSRA brings the best services and offers them in a single marketplace. Below we detail the initial cloud services that CSRA will offer for the MSA. We will add services throughout the life of the contract to keep this solution from becoming stale.

Software as a Service (SaaS)

CSRA will provide the following SaaS offerings:

- Microsoft Office 365
- Microsoft Dynamics CRM Online
- ServiceNow

Microsoft Office 365 for Government with Skype for Business provides a secure and reliable cloud-based Unified Communication Services solution. The solution is managed in accordance with NIST standards for cloud computing and meets the FedRAMP security standards, as it is run by US Citizens in US-only data centers with enhanced security controls. Security of customer's data is a priority, and Office 365 will contractually commit to protect agency data. At the government's discretion, onboarding support services are available to assist in migrating to Office 365 for Government for Unified Communication Services. Microsoft has also developed Office 365 to provide physical, administrative, and technical safeguards to help our customers comply with HIPAA and enables CSRA and Microsoft to sign a HIPAA Business Associate Agreement (BAA).

Microsoft Dynamics CRM Online is a full-service customer relationship management (CRM) application that provides a complete suite of powerful marketing automation, sales force automation and customer service capabilities, all with a familiar user interface based on Microsoft Outlook. Dynamics runs natively within Outlook or within a modern Internet browser as a Web application. Dynamics is also a platform for extended CRM (xRM) solutions that allow Purchasing Entities to manage the interactions and relationships with citizens, employees, partners, suppliers, distributors and vendors. Dynamics can be configured for these extended CRM/ERP/HCM scenarios to enhance the value of all relationships, and improve the ability of agencies to deliver their missions.

ServiceNow Business Management solutions extend visibility so Purchasing Entities can manage people, projects, compliance, and vendors. Consolidate business data to manage demand, understand costs, use resources, execute on projects, ensure regulatory compliance, and manage business relationships.

Platform as a Service (PaaS)

CSRA will provide the following PaaS offerings:

- AppWorks
- ARCWRX

AppWorks and ARCWRX offerings accelerate Agile adoption through preconfigured, pre-integrated Application Lifecycle Management (ALM) platforms, training and coaching.

AppWorks is a CSRA ALM offering and comprises the following:

- **AppWorks Open:** Open Stack ALM development platform: Pre-integrated JIRA, Selenium, Chef, Maven, Git, and Jenkins. We use current industry leading products, recognizing the tools change or need to be specialized.
- **Agile Engineering for Government:** This combines CSRA's Agile development best practices with seasoned coaches so customers can adopt the most appropriate Agile method supported by the right tools. CSRA coaches can guide teams through the cultural changes associated with moving to Agile.

ARCWRX is CSRA's FedRAMP certified PaaS solution that allows developers to develop, host and scale applications in a Cloud environment and comprises the following:

- **Web Frameworks:** JBoss Enterprise Application Platform (EAP) and Enterprise Web Server (EWS), PHP scripting language, programming languages (Python, Ruby and Perl), and Node.js runtime environment.
- **Databases:** MongoDB, MySQL and PostgreSQL

- Application Integration Services: An API Gateway that allows developers to securely connect mobile and Web applications to Web services

Infrastructure as a Service (IaaS)

CSRA will provide the following IaaS offerings:

- Amazon AWS
- Amazon AWS GovCloud
- Microsoft Azure Government Cloud
- CSRA Autonomic Resources ARC-P

Amazon Web Services (AWS) offers a broad set of global compute, storage, database, analytics, application, and deployment services that help organizations move faster, lower IT costs, and scale applications. The largest enterprises and the hottest start-ups trust these services to power a variety of workloads including: Web and mobile applications, Internet of Things, data processing and warehousing, storage, and archive. AWS GovCloud offers additional security accreditations and restricts the user base to government agencies.

Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and Web. It supports the broadest selection of operating systems, programming languages, frameworks, tools, databases and devices. It can run Linux containers with Docker integration; build apps with JavaScript, Python, .net, PHP, Java and Node.js; build back-ends for iOS, Android and Windows devices. Azure cloud service supports the same technologies developers and IT professionals trust.

The CSRA **ARC-P GCC** (Government Community Cloud) provides customers physical or virtual machines in a shared government-only FedRAMP authorized cloud stack. Customers can also have dedicated resources within the ARC-P GCC solution. ARC-P GCC is an IaaS cloud system with customizable virtual machine templates to meet application needs. ARC-P GCC supplies elastic compute resources on-demand from ARC-P compute pools residing in our CONUS-only data centers. ARC-P GCC can support large numbers of agency virtual machines with the ability to scale services up and down according to agency customers' varying requirements. ARC-P GCC offers additional resources such as a virtual-machine disk image library, persistent block storage, customer virtual network (CVN) separation at layer 2, firewalls, load balancers, and public-facing IP addresses. For cloud environment connectivity, customers can use available ARC-P VPN solutions over the Internet or dedicated carrier clouds and circuits.

ARC-P GPC (Government Private Cloud) offers the same features as ARC-P GCC with additional logical and physical separation for private cloud environments that require a dedicated hardware stack. It can also be installed in the customer's data center.

CSRA will provide all the services listed above through our ServiceNow portal as a cloud broker. This provides clients a range of services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Public and government cloud providers such as Amazon AWS and Microsoft Azure, and CSRA's own FedRAMP-compliant cloud, Autonomic Resources ARC-P provide these services. All these resources can be provisioned from a single-service catalog. As additional services mature in the cloud marketplace, CSRA adds them to our catalog so that its offerings will never be old and stale.

In addition, CSRA can provide interested clients a cloud management platform (CMP) such as the Agility Platform. This will allow clients to manage multiple cloud environments from a single interface. It has the ability to manage AWS, Azure, AppWorks, or private VMWare virtualized environments from a single interface. As depicted in **Exhibit 4-5** below, Agility simplifies the hybrid cloud. It automates the deployment and management of cloud applications, development platforms, and a range of other enterprise cloud services across diverse cloud environments by providing:

- Tools that automatically detect and import virtual machines
- A highly versatile graphical workbench to assemble portable stacks, templates, and multi-tier application blueprints for deployment across hybrid clouds
- A fully governed, self-service portal to access standardized and customizable applications, platforms, and other “as-a-Service” offerings for on-demand deployment
- Comprehensive, extensible, policy-driven governance, compliance, and security
- End-to-end cloud security
- Portability across diverse public and private clouds (including VMware vCloud Director, VMware vCenter, Microsoft System Center, Microsoft Azure, Amazon EC2, Terremark, OpenStack, and Rackspace)
- A single runtime management console with fine-grain visibility into costs, resource consumption, workload performance, and more
- Asset version control and change tracking
- Support for enterprise scale (tens of thousands of workloads)
- Distributed reporting architecture
- Application release automation
- Visual dashboard of the entire release pipeline, with the ability to promote software releases and environments via a drag-and-drop graphical interface
- Customizable lifecycle stages, approval processes, and quality gates
- Integration into existing tool chains

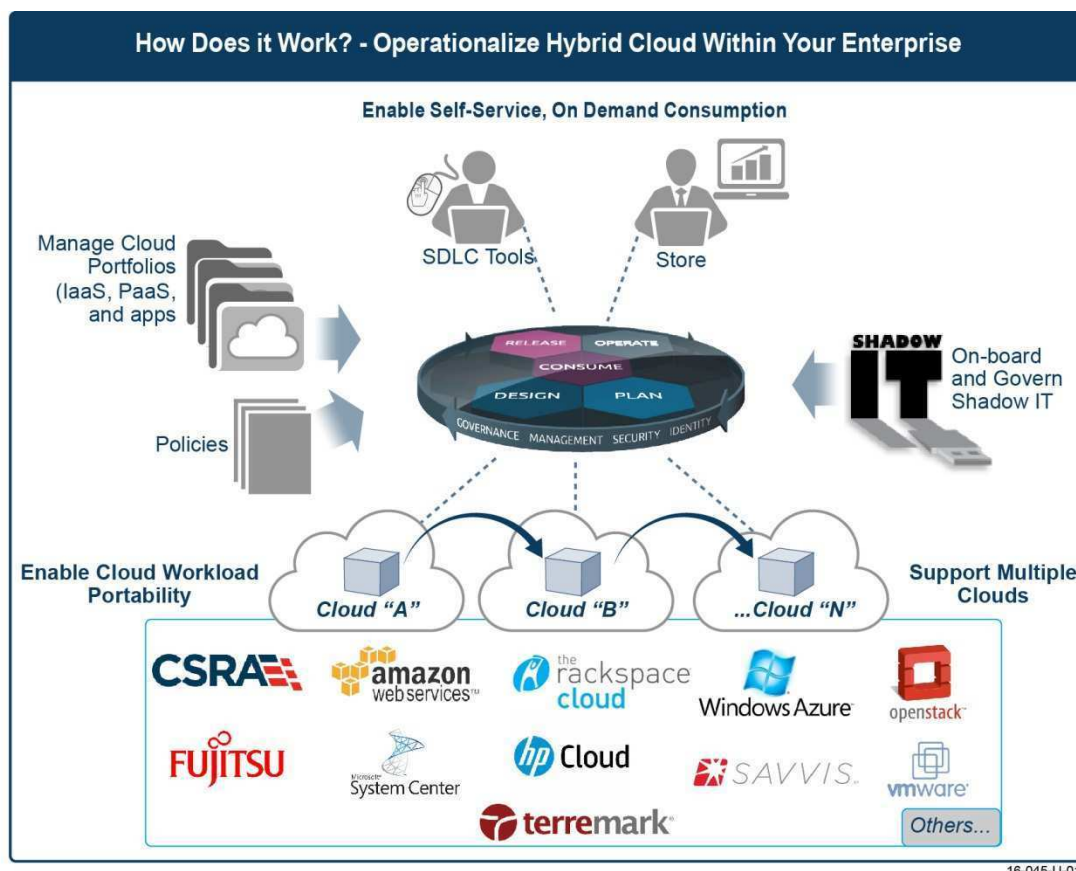


Exhibit 4-5. Hybrid Cloud Management. The Agility Platform simplifies the management of multiple clouds.

4.7 BEST PRACTICES [6.7]

Our FedRAMP-authorized cloud vendors hold many additional attestations and certifications. Their policies and procedures reflect NIST, FedRAMP and other standards with control implementations required to attain and maintain IaaS, SaaS and PaaS cloud certifications. Please refer to Technical Volume **Section 6.6.5**, Third-Party Attestations, Reports and Security Credentials, for additional details. These certifications are required to sell services to state and federal customers. To obtain these certifications, each vendor was independently evaluated before certification award. The achievement of FedRAMP and other certifications are a well-recognized approach to the design, development, management and monitoring built into the policies and procedures each must follow to become accredited. Accreditation drives best practices.

Best Practices

- All vendors are FedRAMP certified
- IaaS/SaaS/PaaS products are standards certified
- Certification attests to vendor compliance
- Accreditations are bench-marked by independent third parties and approved by federal compliance evaluation
- Best practices reflect in each vendors architecture:
 - scalable
 - resilient
 - complies with the key industry standards for security and reliability to provide customers a secure platform

Purchasing Entities that procure services from the cloud vendors assume responsibility for access to sensitive data. Protection for sensitive data is achieved through purchased services or security tools. In general, Purchasing Entities connect their virtual private cloud (VPC) to their data centers using an IPsec hardware VPN connection, making the cloud an extension of their data center. The establishment of an organizational gateway-to-gateway VPN is the most cost-effective method to securely transmit information over the untrusted Internet.

The following sections recap the policies and procedures to provide visibility, compliance, data security and threat protection for cloud-delivered services.

AWS: All AWS customers benefit from a data center and network architecture built to satisfy the requirements of the most security-sensitive organizations. AWS and its partners offer tools and features to help customers meet security objectives around visibility, auditability, controllability and agility. This means that each customer can have the security needed, but without the capital outlay, and at a much lower operational overhead than in an on-premises environment.

AWS's data centers, designed to satisfy the requirements of our most security-sensitive customers, house the AWS cloud infrastructure. The AWS infrastructure provides the highest availability while putting strong safeguards in place regarding customer privacy and segregation. When deploying systems in the AWS Cloud, AWS helps by sharing the security responsibilities with each customer. AWS manages the underlying infrastructure, and customers secure anything deployed in AWS.

Each certification means that an auditor has verified that specific security controls are in place and operate as intended. Customers can view the applicable compliance reports by contacting our CSRA AWS account representative. For more information about the security regulations and standards with which AWS complies, please see the AWS Compliance webpage above. To help meet specific government, industry, and company security standards and regulations, AWS provides certification reports that describe how the AWS Cloud infrastructure meets the requirements of a list of global security standards, including: ISO 27001, SOC, the PCI Data Security Standard, FedRAMP. For more information about the security regulations and standards with which AWS complies, see the AWS Compliance webpage.

Microsoft Azure: To demonstrate that security controls deliver compliance, Microsoft enterprise cloud services are independently validated through certifications and attestations, as well as third-party audits. In-scope services within the Microsoft Cloud meet key international and industry-specific compliance standards, such as ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1 and SOC 2. They also meet regional and country-specific standards and contractual commitments, including the EU Model

Clauses, UK G-Cloud, Singapore MTCS, and Australia CCSL (IRAP). In addition, third-party audits, by firms like the British Standards Institution and Deloitte, validate the adherence of our cloud services to the requirements these standards mandate.

Ultimately, it is up to each customer to determine whether Microsoft services comply with the laws and regulations applicable to the customers' business and legal requirements. To help make these assessments, Microsoft supplies the specifics about its security and compliance programs, including audit reports and compliance packages. Purchasing Entities can verify implementation of the controls by requesting audit results from the certifying third parties or through our Microsoft account representative.

ARC-P: Policies, standards, baselines, guidelines and procedures based on DoD authorizations govern The ARC-P IaaS and PaaS environments. Actionable organizational policy, functionally implemented through security directives, establishes the cumulative organizational security environment. The result is a heightened security environment enforced by cleared, certified personnel using FICAM complaint access management. The ARC-P IaaS and PaaS computing components are administered using FedRAMP-approved VPN remote access. VPN connectivity to customer applications is a capability of private and dedicated application hosting offerings. Remote access VPN connectivity can be provided based on the OpenVPN server platform for end users or standard IPsec site-to-site VPN tunnels established from the ARC-P portal. The customer is not prevented from customizing remote access within their application containers in addition to using the provided SSH access method.

In summary, each cloud vendor is FedRAMP certified and through this method of accreditation, state and federal agencies are increasingly migrating systems to the cloud. As a best practice, Purchasing Entities need to consider the technical abilities of integrators and service offerings required to secure their data and how these elements impact the pricing of a cloud providers' proposed services.

Section 5: Organization Profile [7]

CSRA's contract management approach has four major components: (1) MSA Management and Administration, (2) Order Response and Execution, (3) Marketing and Outreach, and (4) Product R&D and Management. For each component, we address NASPO and Participating Entity collaboration, tools, automation, processes, structure, and quality as shown in **Exhibit 5-1**.

MSA Management and Administration	Marketing and Outreach	Order Response and Execution	Product R&D
1. Collaboration with NASPO and Participating Entities			
Regular meetings and status reports	Regular status meetings Sales calls and follow-up (Participating Entities)	Order Q&A and discussions Status reports and meetings	Product briefings and demos Product roadmap briefings
2. Processes, tools, automation – standard methods and tools for consistency and responsiveness			
Business operations (contracts, finance, subcontracts, and security)	Account plans Salesforce.com (opportunity tracking) Opportunity distribution / tracking system Internet presence	Standard templates: pricing, proposals, and transition PMBOK-based task management process NASPO mailbox	Offering lifecycle management process R&D test bed environment Product/offering configuration control Strategic sourcing
3. Structure – CSRA's Contract Manager coordinates all activities			
Lead: CSRA Contract Manager	Lead: CSRA industry account managers Joint marketing with industry partners	Lead: CSRA assigned project managers CSRA service delivery manager	Lead: CSRA brand manager (IaaS, PaaS, and SaaS)
4. Quality focus – CSRA delivery assurance reviews provide objectivity and independence			
On time, accurate, and complete reports, invoices, and payments	Number of opportunities Dollar value of pipeline Coverage of major agencies	Number of bids and wins Schedule, SLAs, and QASP Rapid issue resolution	New product introduction Customer feedback Product defect and correction metrics

Exhibit 5-1. Contract Management Approach. Our four-part contract management approach achieves collaboration, accountability, responsiveness and quality.

Collaboration

As shown in **Exhibit 5-1**, we collaborate with NASPO and participating entities to achieve program success. We share status data, discuss plans for the future, review performance (including client satisfaction and quality metrics), and discuss actions on issues and risks.

Contract Management to Produce and Deliver Timely IT Commodities and Solutions.

The CSRA NASPO Contract Management Office is located in Huntsville, AL. Our Contract Manager, Jerome Scherzinger, will be the main point of contact for administration, coordination, performance monitoring, and reporting for the MSA. Mr. Scherzinger has full organizational support across the entire CSRA state and local team, CSRA cloud offering leads, CSRA project managers, and CSRA human resources contracts and legal team. **Exhibit 5-2** depicts the CSRA organization supporting Mr. Scherzinger on the NASPO ValuePoint Cloud MSA.

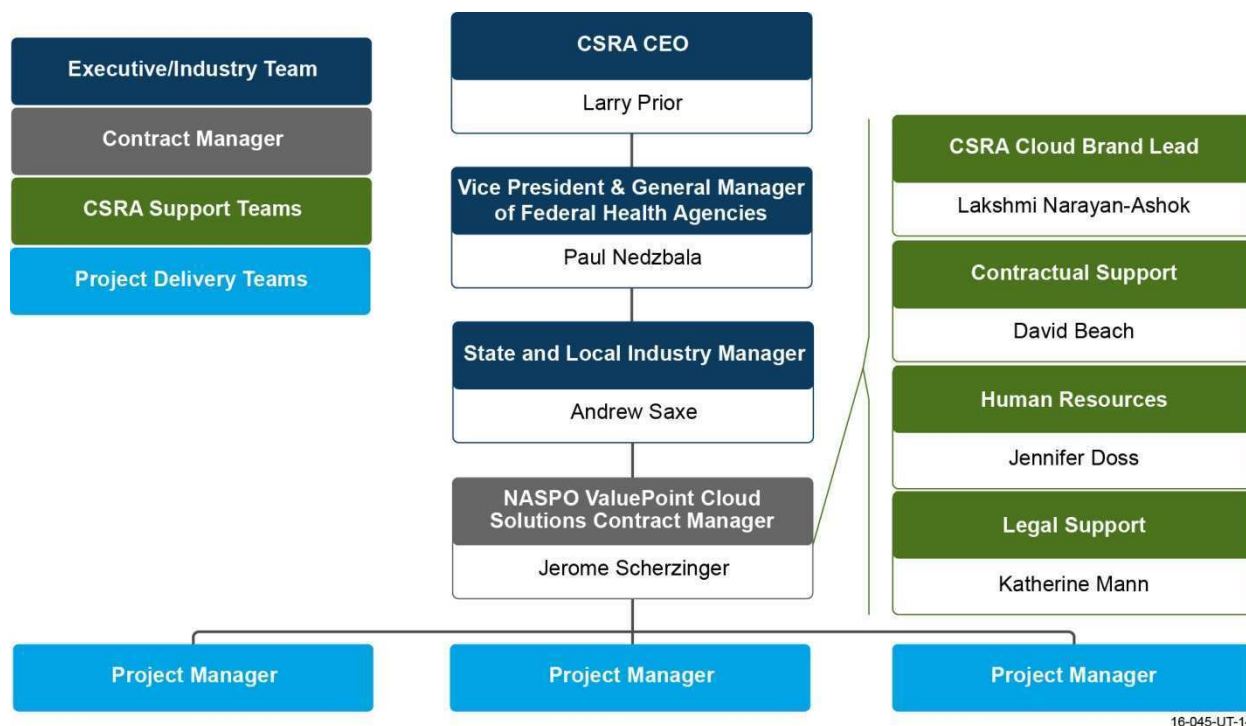


Exhibit 5-2. Contract Support Structure. MSA Contract Manager has direct access to the expertise and support required to provide excellent service to our state and local customers.

Processes and Structures in Place to Support the NASPO ValuePoint Cloud MSA

CSRA account teams call on Participating Entities to identify opportunities early so we can increase our understanding of requirements and possible solutions. Our automated RFP tracking system captures, distributes, tracks, and reports on order requests. It directs orders to the responsible agency account team and technology leader—and confirms that the decision maker has responded. After a bid decision is reached, we form a team (with members from business development, engineering, pricing, contracts, and the Contract Manager) to outline, draft, review, refine, and submit our proposal. No-bid decisions are analyzed to identify actions that boost our bid rate.

Identifying, Mitigating, and Controlling Risks

CSRA’s continuous risk management methodology includes engaging government and CSRA staff to encourage contract-level and specific order stakeholders to identify risks early. We work with the Purchasing Entity to analyze the likelihood and impact of each identified risk. We then develop alternative mitigations, select the best, and implement and track results. We retire a risk only after the Purchasing Entity and CSRA agree that mitigation has been successful (closed loop process). Our organizational structure and tailored, proven processes based on our extensive cloud integration experience help control risks. In addition, adherence to contract scope, an experienced Contract Manager, and IaaS, PaaS, and SaaS technology leadership minimize risk. On each order, the project manager leads risk management actions. Our Contract Manager monitors risk activities and takes the lead on contract-level risks.

Tools and Automation to Support the NASPO ValuePoint Cloud MSA

Exhibit 5-3 summarizes the CSRA tools and automation to support this MSA and the NASPO Cloud MSA mailbox that will be put in place upon award.

Tool / Automated Capability	Value to NASPO and Participating Entities	In Place?
Salesforce.com	- Better opportunity tracking drives work to MSA - Improved preparation for RFP response	Yes
RFP Tracking System	- Increased bid rate - Faster decisions for high quality proposals	Yes
Templates for Pricing, Schedule, Transition	Realistic project plans, faster project startup	Yes
Purchasing/Supply Chain Management	Hardware product availability for multiple orders	Yes
Automated “as a Service” Test and Check	Rapid verification of readiness for transition	Yes
NASPO ValuePoint Cloud Online Service Catalog	Improved customer communications	Within 30 days of contract award

Exhibit 5-3. Contract Management Tools and Processes. *Our comprehensive tools and automation increase responsiveness and quality.*

5.1 CONTRACT MANAGER [7.1]

For the role of Contract Manager, CSRA is proposing D. Jerome Scherzinger, II. He has been with the company for over 24 years and has a total of 37 years’ experience in federal, state, and local government contracting, with 18 of those years specifically as a Contract Manager. He has administered and/or managed contracts involving Cloud Based Services for state contracts that were of similar size and scope to the NASPO ValuePoint Cloud Solutions effort. Specifically, for the last 6 years, a \$102.6 million contract for the State of Alabama that delivered Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), and a 5-year, \$72 million contract for the State of California that delivered Email as a Service (EaaS) to the client.

5.1.1 Contact Information for Contract Manager [7.1.1]

D. Jerome Scherzinger

Office Phone: 256.799.3567

Cell Phone: 256.529.8368

Fax Number: 256.799.4216

Email Address: Jerome.Scherzinger@csra.com

Normal work hours: 8:00 am to 5:00 pm Central Standard Time

5.1.2 Detailed Resume and Description of Contract Manager’s Experience [7.1.2]

D. JEROME SCHERZINGER, II	
Current Position: Manager of Contracts, CSGov Civil and State and Local Agencies	Years at CSRA: 24
Professional Summary	
37 years of experience in federal, state, and local government contracting, with 30 years as a contract administrator/manager, and as a Contract Manager for the last 18 years - Has managed all types of contracts, including numerous Indefinite Delivery Indefinite Quantity (IDIQ) contracts with multiple Task Orders (TOs), and contracts involving cloud based computing services for state clients - Supervised contract administrators using a distributed management model to accommodate their various geographical locations - Interfaces directly with CSRA executive management, and currently manages a contract portfolio in excess of \$2.46 billion - Ensures that his team administers contracts in accordance with all contract, internal reporting, compliance, and risk identification-mitigation requirements; and adhere to all contract requirements and company policies and procedures - Participates in proposal and negotiation activities as proposal volume manager, author, subject matter expert (SME), and advisor - Mentors new and existing employees on CSGov tools, processes, and contracts administration - Member of the National Contract Management Association (NCMA) since 1987	

D. JEROME SCHERZINGER, II

- Five years of experience in local government includes having served as Deputy and then Chief Probation Officer for the Washington Circuit Court, Criminal Division, in Salem, IN

Education and Certifications

Bachelor of Arts, Political Science (major), and Psychology (minor), Indiana University, 1981

Working knowledge of the FAR, DFAR, FIRM, and NASA, NOAA, and EPA FAR supplements as well as procurement procedures for various states throughout the country

Relevant Work Experience

01/1998 – Present	Manager of Contracts	CSC Government Solutions LLC (CSGov), formerly CSC, Huntsville, AL
As Manager of Contracts for CSGov Civil Agencies and CSC State and Local Solutions LLC, directly manages five senior contract administrators located across four states. For CSGov's Defense Industry, managed staff located across seven states and Washington, DC. • Directly interfaces with CSGov executive management regarding a portfolio that includes High Performance Computing (HPC) and cloud based services contracts similar in size and scope to this effort. Performed on contracts for the States of California and Alabama, and advised on other state contracts. Federal government contracts include the Environmental Protection Agency (EPA), Federal Aviation Administration (FAA), Department of Education (ED), National Oceanic and Atmospheric Administration (NOAA), National Aeronautics and Space Administration (NASA), and Department of Energy (DOE). Total portfolio contract value (Federal and State) is approximately \$2.46 billion. • Responsible for direct contract administration, as well as all activities of his team's portfolio. Ensures all policies and procedures, contract requirements, internal reporting, compliance issues, risk identification-mitigation, and contract reviews are conducted in accordance with contract requirements and company policy. In addition, performs contract administration and advisory functions for several federal, state, and local contracts, including: • 10 years as Contract Administrator on a professional services contract for the State of Alabama. The service contract had a fixed billing schedule, and totaled approximately \$102M. Currently, the contract involves networking (about 60%) and distance learning. It began as an HPC, software, and tools development contract delivered under the following cloud based services— SaaS, IaaS, and PaaS. Manager for the State of California Email System (CES) IDIQ contract with multiple Task Orders totaling \$72M delivering Email as a Service (EaaS). • Advisor to the contract administrator on the State of Maryland Coordinated Highways Action Response Team (CHART) program. This IDIQ contract with Work Orders issued on a time and materials (T&M) or firm fixed price (FFP) basis totaled approximately \$57M. • CSGov federal contracts include: – NASA Supercomputing Support Services (NS3) supporting the 5th largest supercomputer in the world. This cost-plus-award fee (CPAF) contract is worth \$594M. – NOAA High Performance Computer Research and Development performance based contract worth \$371M and involving acquisition, installation, operations, and maintenance. This contract's distributed computing environment includes laboratories and centers in CO, NJ, MD, and WV. NOAA HPC is an 8-year effort valued at more than \$371M, staffed by 15 full-time employees who provide support to 1,000+ users. – Previous clients include the US Army Redstone Arsenal in Huntsville, AL; Simulation, Training and Instrumentation Command (STRICOM) in Orlando, FL; Missile Defense Agency in Fort Belvoir, VA and Huntsville AL; Ft. Huachuca in Arizona; White Sands Missile Range in New Mexico, and Boeing in Seattle, WA.		
05/1995 – 01/1998	Member of Technical Staff	Nichols Research Corporation, Huntsville, AL
Served as the liaison between Technical Operations and the Contracts office. Coordinated and tracked all new business activities for the HPC Business Segment and participated in various proposal teams as both a section writer and a volume manager.		
05/1991 – 05/1995	Senior Contract Administrator	Northrop Grumman Corporation, Huntsville, AL
Contracts administration support on the proposal before award, and on the project after award, for the NASA Engineering Analysis and Data System (EADS) Supercomputer contract (EADS II) at Marshall Space Flight Center, Alabama.		

D. JEROME SCHERZINGER, II		
08/1990 – 05/1991	Senior Contract Administrator	SCI Systems Inc., Huntsville, AL
Managed approximately \$95M in production contracts (both design and build to print). Clients included the US Army and various commercial entities.		
04/1984 – 08/1990	Contract Administrator	Computer Sciences Corporation (CSC), Huntsville, AL
Administrator of cost-plus fixed fee (CPFF) level-of-effort (LOE), time and materials (T&M), CPFF Completion, FFP, IDIQ, and Letter contracts at Redstone Arsenal. (January 1987 – August 1990, Huntsville, AL) Data Manager (October 1985 – January 1987 Huntsville, AL) Security/Facilities Administrator (April 1984 – October 1985 Dayton, Ohio)		
07/1979 – 04/1984	Chief Probation Officer/Deputy Probation Officer	Washington Circuit Court, Criminal Division, Salem IN
Chief Probation Officer for the Washington Circuit Court, Criminal Division, in Salem, IN (January 1982 – April 1984). Deputy Probation Officer for the same court (July 1979 – April 1982).		

5.1.3 Contract Manager's Roles and Responsibilities [7.1.3]

The CSRA Contract Manager is the single point of coordination across the program lifecycle. He oversees acquisition and delivery and ensures reliability and consistency across all CSRA projects for NASPO ValuePoint Cloud. The Contract Manager is responsible for collaboration between CSRA, NASPO and participating entities, and has the following responsibilities:

- **Contract Management and Administration (including business operations):** Regular meetings and email/telephone contacts on overall status, performance, and action items; NASPO mailbox; attendance at contract events; preparation of invoices and resolution of any issues
- **Order Response and Execution (based on RFP requirements):** Formal dialog with NASPO and participating entities during the proposal process; kick-off meetings; daily meetings during start-up/transition (status, issues); monthly meetings/reporting on performance (product delivery, schedule, budget, quality); and close-out at completion
- **Marketing and Outreach:** Review overall and account-specific plans; sales calls and follow-ups to present and identify/understand end-customer needs and possible solutions; joint sales calls and sharing opportunity-specific information with NASPO; promote NASPO within CSRA
- **Product R&D (Technical Innovation):** Review product roadmap (provide feedback); discuss new products to be added to the contract; participate in NASPO strategic sourcing initiatives; review planned product changes (e.g., price reductions, increased capabilities)

Order kick-offs are especially important in promoting collaboration in program execution. Within one week of order award, our Contract Manager will assign a project manager and conduct a kick-off meeting with government stakeholders. At the kickoff meeting, we begin to build effective relationships and discuss project-specific roles and responsibilities, schedule, milestones (including an operational readiness review), communications, transition/start up, resources, and SLAs/metrics.

Additional Strategic Responsibilities

- Point-of-contact to help resolve issues and perform other functions that may arise relating to the contract and its task orders
- Promote, educate and train on the NASPO ValuePoint Cloud MSA contract to government through participation in trade shows, conferences, and other meetings where potential customers have a significant presence
- Provide all required reporting information accurately and in a timely manner
- Primary focal point within CSRA on all matters pertaining to NASPO ValuePoint Cloud MSA

Additional Tactical Responsibilities

- Monitor BidSync, and remain involved in all phases of the order. Distribute orders and requests to the correct operational area within CSRA. Submitting questions and proposals
- Periodic meetings with each task order Project Manager. Project Managers pro-actively inform the Contract Manager of possible risks and issues, particularly when program-level attention is needed
- Monitor quality assurance and coordinate delivery of contractual deliverables, e.g. monthly technical and financial status reports, usage metrics, and invoices for compliance with the contract vehicle
- Initial point of contact for interpreting and resolving contract related issues on a task. Project Managers will perform day-to-day operational informational interchange with the government customer
- Help develop proposals through sharing of information, examples and discriminators
- Meet with the customer, CSRA Project Manager and staff for a task order kick-off meeting at the initiation of each task order.
- Verify Contracts Database Record and distribute Flash Report upon the award of the task. The database record contains a summary of the negotiated work to be accomplished and the agreed upon price. Upon award of a task, meet with the representative of the performing Group/Division(s) to establish an understanding of how contractual issues will be addressed
- Upon award of the MSA, meet with the Program Control Office (PCO) in the performing business area and establish an understanding of how Program Control issues will be addressed. Ensure that PCO, accounting, and billing staff understand the requirements for timely status reports and invoices and inform them of the timelines and data to be transmitted for the monthly status reports and invoices
- Help project managers resolve issues related to task order delivery, and enforce processes that support delivery of high quality
- Perform regular liaison with project managers, and maintain currency on project progress and status
- Enforce quality assurance processes for quality review and ensure deliverables comply with task requirements

Section 6: Technical Response [3.12 (6), 8]

Assessment of Cloud Solutions Provided [3.12 (6) (A)]

CSRA, an industry-leading systems integrator and cloud broker, provides a full suite of cloud services to state, local, federal, Department of Defense, and intelligence agencies. Services range from building and managing private clouds to migrating customers to the cloud at a fixed price. Our experience with large agencies has taught us that one solution does not fit all. Recognizing that each department within an agency has unique requirements, CSRA carefully selects and integrates cloud solutions that provide operational efficiencies and synergies.

CSRA's cloud broker model provides a single, consistent interface for our customers to access cloud service providers (CSPs). It also provides a mechanism to make cloud workloads portable across various CSPs. According to the National Institute of Standards and Technology (NIST), cloud brokers provide services in three categories:

- **Service Intermediation** – The broker provides a value-add to one or more services a CSP offers (e.g., additional security, identity management).
- **Service Aggregation** – The broker bundles and integrates services from multiple CSPs into one or more new services, including all integration necessary and data movement among CSPs.
- **Service Arbitrage** – The broker provides aggregated services, but the CSPs providing the underlying services may vary based on factors such as cost and performance.

Our solution combines CSRA's Autonomic Resources Cloud Platform (ARC-P) with Amazon Web Services (AWS) and Microsoft Azure FedRAMP certified cloud offerings, and drives value for Participating Entities by fostering price competition. CSRA's solution has the flexibility to add or remove any IaaS, SaaS or PaaS solution—allowing Participating Entities to take advantage of emerging solutions over the next 10 years. By providing competing products, we ensure that customers are not locked in to any one product. CSRA's cloud offering provides the services needed to make customers successful in the cloud. As depicted in [Exhibit 6-1](#), CSRA offers migration services; and our Integrated Technology Center (ITC) in Bossier City, LA provides help desk, network operations center (NOC), and security operations center (SOC).

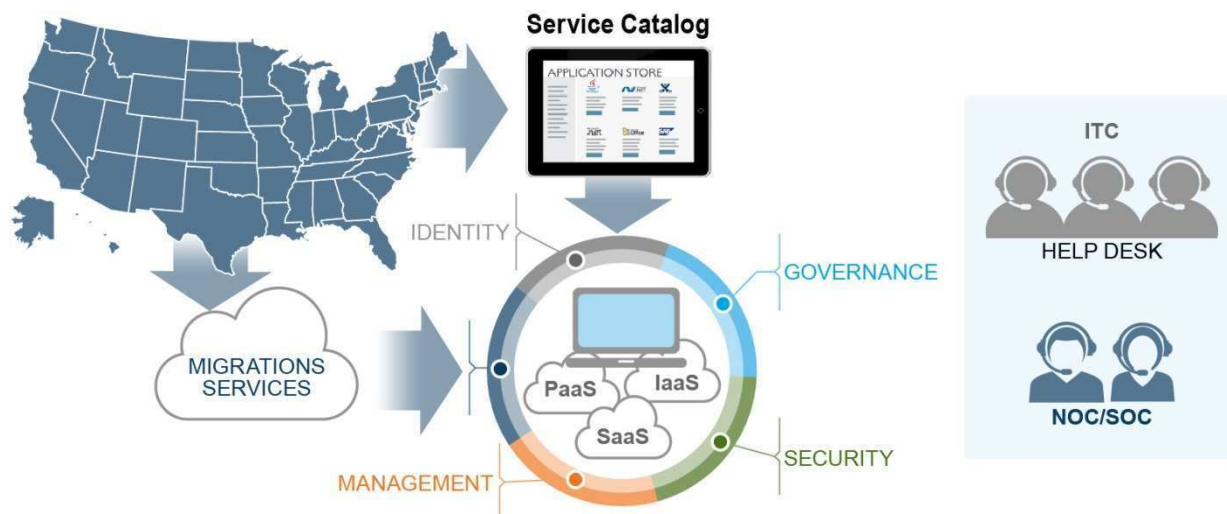
Our lessons learned and successes implementing government agency infrastructures and end-user services programs, give us insight into customer challenges and an understanding of their specific requirements and procedures. We build on this experience to meet requirements while minimizing risk, controlling costs, and implementing an optimal cloud service solution that leverages:

- CSRA's experience managing data centers
- Teammates and technology partners to lead Participating Entities through planned data center consolidations and cloud migrations
- A network of strategic global alliances with AWS, Microsoft, VMware, EMC, IBM, Oracle, and many other technology leading firms
- FedRAMP certified CSPs in AWS, Microsoft Azure, and CSRA ARC-P

CSRA uses an enterprise IT governance approach and architecture model to support the solution and enterprise roll out of the cloud technologies. Our proposed solution and technical approach align with the NIST Cloud Strategy and Vision, including complete lifecycle support for cloud processes to deliver a streamlined IT delivery.

CSRA's Proven Cloud Expertise

- **DHS** – CSRA built one of the first government-owned contractor-run Federal Information Security Management Act (FISMA) moderate private clouds
- **FAA** – CSRA is a cloud broker for AWS and Azure services
- **Autonomic Resources**, a CSRA company, built the first FedRAMP certified community cloud, ARC-P



16-045-U-013

Exhibit 6-1. CSRA Concept of Operations. *Participating Entities use the CSRA Service Catalog to order service in the cloud or use our migration services to move existing services to the CSRA solution.*

Our solution offerings satisfy all the key concepts and characteristics of cloud services, per the NIST Special Publications 500-292 and 800-145, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

The initial cloud services CSRA will offer for the MSA are listed below. We will add services throughout the life of the MSA:

Software as a Service (SaaS)

CSRA provides the following SaaS offering: Office 365, Microsoft Dynamics CRM Online, and ServiceNow.

Microsoft Office 365 for Government with Skype for Business provides a secure and reliable cloud-based Unified Communication Services solution managed in accordance with NIST standards for cloud computing, and compliant with FedRAMP security standards. The security of Entities' data is a priority, and we commit to protect agency data. At the Entity's discretion, onboarding support services are available to assist in migrating to Office 365 for Government for Unified Communication Services. Office 365 also provides physical, administrative, and technical safeguards to help customers comply with the Health Insurance Portability and Accountability Act (HIPAA); and enables CSRA and Microsoft to sign a HIPAA Business Associate Agreement (BAA).

Microsoft Dynamics CRM Online is a full-service customer relationship management (CRM) application that provides a complete suite of powerful customer service capabilities, and marketing automation, and sales force automation with a familiar user interface based on Microsoft Outlook. Dynamics runs natively within Outlook or within a modern Internet browser as a Web application. It is also a platform for extended CRM (xRM) solutions that manage interactions and relationships with citizens, employees, partners, suppliers, distributors, and vendors. Dynamics can be configured for xRM, ERP, and human capital management (HCM) scenarios to enhance the value of all relationships and improve the ability of agencies to deliver their missions.

ServiceNow Business Management solutions extend visibility and allow customers to manage people, projects, compliance, and vendors. Business data is consolidated to effectively manage demand, understand costs, use direct resources, execute projects, ensure regulatory compliance, and manage business relationships.

Platform as a Service (PaaS)

CSRA provides the following PaaS offering: AppWorks and ARCWRX.

Our **AppWorks and ARCWRX offerings** accelerate Agile adoption through preconfigured, pre-integrated Application Lifecycle Management (ALM) platforms, training and coaching. AppWorks comprises:

- AppWorks Open: Open Stack ALM development platform: Pre-integrated JIRA, Selenium, Chef, Maven, Git, and Jenkins. We use industry leading products, customizing or updating them as required.
- Agile Engineering for Government: Combines CSRA's Agile development best practices with seasoned coaches enabling our customers to adopt the most appropriate Agile method supported by the right tools. CSRA coaches are available to guide teams through the cultural changes associated with moving to Agile.

ARCWRX, CSRA's FedRAMP certified PaaS solution, allows developers to develop, host and scale applications in a cloud environment. It comprises:

- Web Frameworks: JBoss Enterprise Application Platform (EAP) and Enterprise Web Server (EWS), PHP scripting language, programming languages (Python, Ruby and Perl), and Node.js runtime environment.
- Databases: MongoDB, MySQL and PostgreSQL
- Application Integration Services: An API Gateway that allows developers to securely connect mobile and Web applications to Web services.

Infrastructure as a Service (IaaS)

CSRA provides the following IaaS offerings: AWS, AWS GovCloud, Microsoft Azure Government Cloud, and CSRA ARC-P.

AWS offers a broad set of global compute, storage, database, analytics, application, and deployment services that help organizations move faster, lower IT costs, and scale applications. Large enterprises trust these services to power a variety of workloads, including Web and mobile applications, Internet of Things, data processing and warehousing, storage, and archive. AWS GovCloud offers additional security accreditations and restricts the user base to government agencies.

Azure is a growing collection of integrated cloud services—analytics, computing, database, mobile, networking, storage, and Web. It supports the broadest selection of operating systems, programming languages, frameworks, tools, databases and devices. It can run Linux containers with Docker integration; build apps with JavaScript, Python, .net, PHP, Java and Node.js; and build back-ends for iOS, Android and Windows devices.

The CSRA **ARC-P GCC** (Government Community Cloud) provides customers with physical or virtual machines (VMs) in a shared government-only FedRAMP authorized cloud stack. Customers can also have dedicated resources within the ARC-P GCC solution. ARC-P is an IaaS cloud system with customizable VM templates to meet application needs. ARC-P IaaS supplies on-demand elastic compute resources from ARC-P compute pools residing in CSRA's continental US-only data centers. ARC-P supports large numbers of agency VMs with the ability to scale services up or down depending on requirements. ARC-P IaaS offers additional resources such as a virtual-machine disk image library, persistent block storage, customer virtual network (CVN) separation at Layer 2, firewalls, load balancers, and public-facing IP addresses. For cloud environment connectivity, customers can use available ARC-P VPN solutions over the Internet or dedicated carrier clouds and circuits.

ARC-P GPC (Government Private Cloud) offers the same features as ARC-P GCC with additional logical and physical separation for private cloud environments that require a dedicated hardware stack. It can also be installed in a customer's data center.

CSRA constantly evaluates new services to see if they offer benefits for our customers. Other services CSRA will evaluate to add to this marketplace include Google Cloud, VMWare vCloud Air, and Salesforce.

Understanding of the Technical Requirements

CSRA has provided the same service models to the State of California, the City of Los Angeles, DHS, FAA, Department of State (DoS), Administrative Office of the US Courts, and NASA Jet Propulsion Laboratory (JPL). For the City of Los Angeles, we provided IaaS, PaaS, and SaaS to more than 17,000 city employees. These projects confirm that CSRA's approach to project implementation is based on a comprehensive understanding of how stakeholders use systems. Detailed descriptions of these projects can be found in **Section 4.2**.

For more than 12 years, CSRA has provided services from data center virtualization to large cloud services using commercially available community clouds and CSRA-built private clouds. We will apply the experience gained from these cloud services projects to the Participating Entities' needs.

Our approach includes requirements analysis and systems engineering; industry standard Project Management Institute (PMI)-based project management, ITIL, and Capability Maturity Model Integration (CMMI) processes; and use of our proven systems development methodology.

Offeror's Ability and Approach [3.12 (6) (A)]

CSRA's solution provides a cloud marketplace from a single systems integrator that allows Participating Entities to select from an array of service offerings. We provide market-leading solutions such as AWS, Microsoft Azure, and Office 365 complemented by our own products, e.g., ARC-P and ARCWRX, to fill requirements such as on-premises solutions. In addition, CSRA offers value-added services that include help desk, patch management, cloud migration, and cloud management platform (CMP).

The variety of CSPs offered by CSRA allows Purchasing Entities to deploy hybrid clouds, which can be any combination of the cloud services we offer. CSRA recommends cloud broker services, which allow us to provide a single consistent interface for the Entities to manage, govern and access CSPs. The interface can serve either business or technical purposes; also provides a mechanism to make cloud workloads portable across the varied CSPs.

With the Agility CMP, CSRA can provide broker services among virtualized environments, and community, public, and private clouds. This protects investments the Purchasing Entity has already made in hardware, and allows them to tie into one seamless interface. CSRA successfully employed this cloud broker approach for the FAA.

Necessary Resources [3.12 (6) (A)]

CSRA, one of the largest US government systems integrators, has extensive relevant experience and reach-back capabilities to subject matter experts. We are currently providing similar services to large government organizations such as the FAA and DHS. Additional details on these projects are provided in Section 4.2.

6.1 TECHNICAL REQUIREMENTS [8.1]

6.1.1 Identification of Cloud Service and Deployment Model(s) [8.1.1]

CSRA's cloud broker service model allows us to provide IaaS, PaaS, and SaaS. Public and government cloud providers such as AWS, Microsoft Azure and CSRA's FedRAMP-compliant cloud—Autonomic Resources ARC-P—provide these services, which are available in the following deployment models:

- Public – Open to all Internet users
- Community – Open to US government agencies only
- Private Off Premises – Cloud dedicated to one customer located in vendor facilities
- Private On Premises – Cloud dedicated to one customer located in customer facilities

All these resources can be provisioned from a single service catalog and management interface, which allows us to provide the best solution for each Purchasing Entity, including a hybrid approach that combines any or all of the solution's components. CSRA can easily update our offerings to keep pace with the industry and Participating Entities' needs. CSRA's initial cloud services and their deployment models include:

SaaS

- Office 365 – in a community cloud deployment model
- Microsoft Dynamics CRM Online – in a community cloud deployment model

PaaS

- AppWorks in a community cloud deployment model
- AppWorks in a private cloud deployment model
- ARCWRX in a community cloud deployment model
- ARCWRX in a private cloud deployment model

IaaS

- AWS in a public cloud deployment model
- AWS GovCloud in a community cloud deployment model
- Microsoft Azure Government Cloud in a community cloud deployment model
- CSRA ARC-P in a community cloud deployment model
- CSRA ARC-P in a private off premises cloud deployment model
- CSRA ARC-P in a private on premises cloud deployment model

6.1.2 Meeting NIST Essential Characteristics [8.1.2]

As detailed below, CSRA's solution meets the NIST essential characteristics.

6.1.2.1 On-Demand Self Service [8.1.2.1]

CSRA provides our customers with on-demand access to all our services through our automated ServiceNow catalog. This interface is available 24x7 to allow customers to request support or provision or de-provision services.

6.1.2.2 Broad Network Access [8.1.2.2]

All resources are available through the ServiceNow Web interface and can be accessed with a modern Web browser such as Internet Explorer 9 or greater, Safari 6.1 or greater, Firefox 31 or greater, and Chrome 39 or greater on any client device (e.g. smart phone, tablet, or computer).

6.1.2.3 Resource Pooling [8.1.2.3]

AWS, Azure and ARC-P are virtualized multi-tenant environments. ARC-P can be deployed as a dedicated private cloud, which still allows multi-tenancy within a Purchasing Entity's organization.

6.1.2.4 Rapid Elasticity [8.1.2.4]

With an underlying infrastructure of AWS, Azure, and ARC-P, a global cloud infrastructure allows Entities to innovate, experiment, and iterate. Instead of waiting weeks or months for hardware, customers can instantly deploy new applications, scale up as workloads increase, or scale down based on decreased demand. Existing infrastructures can handle spikes in traffic with no interference to normal business operations. Auto-scaling capabilities in the Agility Platform scale resources up to meet unexpected demand, and back down as demand decreases, regardless of whether resources are located on AWS, Azure or ARC-P.

6.1.2.5 Measured Service [8.1.2.5]

The CSRA solution meets the NIST characteristic of measured service for the different offerings. Active user accounts per month measures our SaaS offering. A node per month measures our PaaS offering. For our IaaS offering, VMs are measured by the hour. We measure storage and network usage by gigabyte per month.

6.1.3 Identification of Solution Subcategories [8.1.3]

The CSRA solution contains IaaS offerings, PaaS offerings, and SaaS offerings. We list and categorize our offerings in **Exhibit 6-2**.

Name	Service Model	Service Category
AWS	IaaS	Computer/Infrastructure Services, Storage and Network
ARC-P	IaaS	Computer/Infrastructure Services, Storage and Network
Microsoft Azure	IaaS	Computer/Infrastructure Services, Storage and Network
AppWorks	PaaS	Development, Testing and Deployment
ARCWRX	PaaS	Development, Testing and Deployment
Office 365	SaaS	Office Productivity, Collaboration, Meeting Planning, hosting, and conferencing
Microsoft Dynamics CRM Online	SaaS	Customer Relationship Management
ServiceNow	SaaS	IT Service Management

Exhibit 6-2. Service Categories. *A full range of service categories allow Participating Entities to get all their cloud computing needs from one place.*

As a systems integrator and cloud broker, CSRA constantly adds industry leading products to our portfolio. Over the 10-year term of this MSA, as technology evolves, CSRA’s model allows us to keep pace with change and provide Participating Entities access to leading edge solutions.

6.1.4 Willingness to Comply with Attachments C&D [8.1.4]

CSRA’s IaaS, PaaS, and SaaS service models comply with the NIST definition for those models described in Attachment C.

Our IaaS offerings allow customers to provision processing, storage and networks; and deploy and run selected software, which can include operating systems and applications. Purchasing Entities do not manage or control the underlying cloud infrastructure, but do control operating systems, storage, and deployed applications.

Our PaaS offerings allow Purchasing Entities to deploy customer-created or acquired applications created using programming languages, libraries, services, and tools AppWorks and ARCWRX support onto the cloud infrastructure. Purchasing Entities do not manage or control the underlying cloud infrastructure (including network, servers, operating systems, or storage), but do control deployed applications and configuration settings for the application-hosting environment.

Our SaaS offerings allow Purchasing Entities to use applications running on a cloud infrastructure. Applications are accessible from client devices through either a thin client interface, such as a Web browser, or a program interface. Purchasing Entities do not manage or control the underlying cloud infrastructure (including network, servers, operating systems, storage, or individual application capabilities), with the possible exception of limited user-specific application configuration settings.

As detailed in **Section 6.1.5**, CSRA complies with the requirements of Attachment D.

6.1.5 Offerings Adherence to Attachment D [8.1.5]

CSRA’s solution meets the definitions described in Attachment D.

On-Demand Self-Service

CSRA provides our Purchasing Entities with on-demand access to all of our services through our ServiceNow catalog. This automated interface is available 24x7 to allow customers to provision services, de-provision services, or request support.

Broad Network Access

All these resources are available through a Web interface so they can be accessed by any client device (e.g., smart phone, tablet, or computer).

Rapid Elasticity

With an underlying infrastructure of AWS, Azure, and ARC-P, a global cloud infrastructure allows Purchasing Entities to innovate, experiment, and iterate. Instead of waiting weeks or months for hardware, Purchasing Entities can instantly deploy new applications, scale up as workloads increase, or scale down based on decreased demand. Existing infrastructures can handle spikes in traffic with no interference to normal business operations. Auto-scaling capabilities in the Agility Platform scale resources up to meet unexpected demand, and back down as demand decreases, regardless of whether resources are located on AWS, Azure or ARC-P.

Resource Pooling

AWS, Azure and ARC-P are virtualized multi-tenant environments. ARC-P can be deployed as a dedicated private cloud, which still allows multi-tenancy within a customer's organization.

CSRA's cloud broker service model allows us to provide IaaS, PaaS, and SaaS. Public and government cloud providers such as AWS, Microsoft Azure and CSRA's FedRAMP-compliant cloud—Autonomic Resources ARC-P—provide these services, which are available in the following deployment models:

- Public – Open to all Internet users
- Community – Open to US government agencies only
- Private Off Premises – Cloud dedicated to one Purchasing Entity located in vendor facilities
- Private On Premises – Cloud dedicated to one Purchasing Entity located in Purchasing Entity facilities

All these resources can be provisioned from a single service catalog and management interface, which allows us to provide the best solution for each Purchasing Entity, including a hybrid approach that combines any or all of the solution's components. CSRA can easily update our offerings to keep pace with the industry and the Participating Entities' needs. CSRA's initial cloud services and their deployment models include:

SaaS

- Office 365 – in a community cloud deployment model
- Microsoft Dynamics CRM Online – in a community cloud deployment model

PaaS

- AppWorks in a community cloud deployment model
- AppWorks in a private cloud deployment model
- ARCWRX in a community cloud deployment model
- ARCWRX in a private cloud deployment model

IaaS

- AWS in a public cloud deployment model
- AWS GovCloud in a community cloud deployment model
- Microsoft Azure Government Cloud in a community cloud deployment model
- CSRA ARC-P in a community cloud deployment model
- CSRA ARC-P in a private off premises cloud deployment model
- CSRA ARC-P in a private on premises cloud deployment model

Private Cloud

ARC-P offers the greatest level of security; and can be ordered in a fully dedicated model that allows Purchasing Entities to provision cloud resources without having to share the infrastructure with anyone outside the organization. .

Community Cloud

Three community clouds are available in CSRA's solution: AWS GovCloud, Microsoft Azure Government Cloud, and ARC-P. All three are restricted to US federal, state and local government organizations; and are FedRAMP Moderate-compliant so they provide greater security than public clouds.

Public Cloud

CSRA solution provides access to AWS, which is open to the general public. This provides the lowest rates for provisioning resources with lowest data security requirements. AWS can host public-facing Web servers that have low-risk data; and can also host development environments that require no real data. The CSRA solution contains options to meet each Purchasing Entity's budget and security needs.

Hybrid Cloud

Through a CMP such as CSRA's Agility Platform, Purchasing Entities can provision and manage resources in any of the environments from a single interface. From this single interface, Purchasing Entities can manage their high data-risk resources in the private cloud, medium data-risk resources in the community cloud, and low data-risk resources in the public cloud.

6.2 SUBCONTRACTORS [8.2]

Our initial offering includes CSRA's ARC-P, AWS, and Microsoft Azure for IaaS; CSRA's Agility platform for PaaS management; and a variety of SaaS offerings, which include a range of Microsoft software suites.

6.2.1 Intention to Directly Provide Services or through Subcontract [8.2.1]

As an experienced systems integrator, CSRA brings the best subcontractors to the MSA. As part of our service catalog, we initially offer Participating Entities cloud services from CSRA products and our strategic alliance partners, Amazon and Microsoft. As described in Section 6.2.3, Amazon and Microsoft are the most qualified service providers in the industry.

6.2.2 Description of Use of Contractors [8.2.2]

CSRA offers three IaaS options as part of our service catalog: CSRA's ARC-P platform, AWS, and Microsoft Azure. Purchasing Entities can request the CSRA CSP that best fits their needs; or CSRA may recommend a platform based on our experience and understanding of technical requirements. AWS and Azure are existing CSRA alliance partners so we can provide their services to Purchasing Entities in a transparent manner. Existing catalog services and future offerings will be provided without the need for additional positions.

6.2.3 Subcontractor Qualifications [8.2.3]

AWS and Microsoft Azure were recognized by Gartner in their 2014 Magic Quadrant for Cloud Infrastructure as a Service Report. Both feature appropriate regional support and proven capable compute, storage, network, and security infrastructures.

Gartner describes AWS as having "a diverse customer base and the broadest range of use cases, including enterprise and mission-critical applications. It is the overwhelming market share leader, with more than five times the cloud IaaS compute capacity in use than the aggregate total of the other 14 providers in this Magic Quadrant. It is a thought leader; it is extraordinarily innovative, exceptionally agile, and very responsive to the market. It has the richest array of IaaS features and PaaS-like capabilities, and continues to rapidly expand its service offerings. It is the provider most commonly chosen for strategic adoption."

Gartner describes Microsoft Azure as having, "a vision of infrastructure and platform services that are not only leading standalone offerings, but that also seamlessly extend and interoperate with on-premises Microsoft infrastructure (rooted in Hyper-V, Windows Server, Active Directory and System Center) and applications, as well as Microsoft's SaaS offerings. Its vision is global, and it is aggressively expanding into multiple international markets." Gartner's independent analysis of AWS and Microsoft Azure

underscore their qualifications and ability to provide all IaaS services required to support the NASPO ValuePoint Cloud MSA.

Our relationships with AWS and Microsoft include liaisons and points of contact, service level agreements, performance monitoring, risk mitigation plans, and issue escalation and resolution plans used to validate compliance with all statement of work requirements and remediate any issues. Our Contract Manager has access to the people, processes, and tools required to oversee and validate performance.

6.3 WORKING WITH PURCHASING ENTITIES [8.3]

6.3.1 Working with Purchasing Entities [8.3.1]

Before, During and After Data Breaches – Service continuity and incident management and response are unique provisions of the Cloud Services design. These provisions depend on the incident and where it occurs within the Purchasing Entity’s solution. Each cloud vendor responds to internal incidents within their operating environments with the customer. Cloud vendors manage security of the cloud infrastructure. Purchasing Entities control the security they choose to implement to protect their content, platform, applications and systems. If an incident occurs within a customer-provisioned environment, the customer is responsible for remediation. If CSRA provides an IaaS, SaaS or PaaS environment, we work with the customer to recover from unexpected events such as computing environment failure, data corruption, and intrusions that affect availability, integrity or confidentiality of customer data. The following describes our incident management process.

Incident Response

- Incident Policy: Linking each customer with the cloud vendor and CSRA through problem reporting ensures customer is trained on proper procedure
- Incident Handling: Provided by cloud vendors and CSRA; customer works with cloud vendor or CSRA to resolve major security incidents
- Incident Response Phases: Cloud vendors and CSRA follow established incident management processes
- Debriefing: Provided by cloud vendors or CSRA as a part of the incident handling process

Prior to an Incident: When a Purchasing Entity purchases a CSRA service, we connect them to the CSRA SOC Computer Incident Response Team (CIRT) and cloud vendor cyber incident response personnel. The CSRA CIRT interfaces with customers, their SOC’s or network operations security centers (NOSCs), and their cloud provider technical personnel. The CIRT comprises the SOC manager, analysts from cloud vendors and CSRA, and engineers. If necessary, the CIRT requests personnel from other ITS divisions to assist on the incident response team. Additional personnel may include division managers, engineers, administrators, and on-call personnel.

Establish Customer Relationships: We prepare to support Purchasing Entities by establishing them in our ServiceNow Trouble Ticket System. Problems are reported to the CSRA SOC via the CSRA Help Desk. Standard operating procedures (SOPs) include knowledge and escalation process scripts for handling customer calls. CSRA SOC capabilities include customer service monitoring and Web services that provide statistics and trending analysis of aggregate metrics from sources that may infer a security incident.

We document and track common incidents discovered during system monitoring, including those that do not require the visibility, scrutiny, and level of documentation of high-impact incidents. For serious incidents that have the potential for lengthy outages, we implement an established plan with processes that address preparation, identification, containment, eradication, recovery, and follow-up. The plan details the steps to follow when responding to an IT-related security incident, and includes coordination with the affected customer.

When notified by a Purchasing Entity, or if our monitoring process identifies abnormal traffic, we immediately begin collecting and analyzing information to determine the level of threat posed by the event and the proper response scenario.

During this step, we determine the event’s communication medium and delivery method, physical characteristics, IDS alert message and associated rules; status (past, present, repeating), and affected hosts

(hardware, software, network details). We document all relevant facts regarding active, verified incidents in Request Tracker (RT), the SOC ticket tracking system. This includes assigning the appropriate classifications to the incident.

Incident Response Kickoff: This step begins the response and involves identifying affected systems, analyzing and documenting facts about the incident, and notifying or responding to help desk tickets submitted by affected customers. A Service Restoration Team is assigned to respond to the event. This step may be repeated if additional compromises discovered during the assessment require continuing analysis. An incident progress report with the latest information is prepared for management and leadership. We integrate the appropriate cloud vendor if appropriate.

Customer Notification: Data gathered during the response kickoff may include user and system information, external point of contacts, and the direction of the “attack” (i.e., antagonist and suspected target). Information on persons, projects, and affected customers may be requested from the contracts department. The CSRA SOC is made aware of IT support teams related to the project or customer-specific compliance directives with definitive POC lists.

Document Incident Findings: The SOC Record Tracker is the official record for incident tracking. Incident details are stored in the corresponding incident ticket.

Impact Analysis and Containment: For major incidents, the analysis stage is the most resource intensive. This stage may involve acquiring and analyzing logs, and forensic analysis of tools on the network. Based on the results, responders create a list of indicators they can use to identify malicious activity on the network. Identifying additional compromises can take time so all confirmed incidents are handled with the utmost urgency. Based on results from indicators of compromise (IOCs), analysts verify the alerts that indicate a compromise. If additional compromises are discovered, the process returns to Kickoff, to re-evaluate affected parties and systems. We provide these impact assessment results as an incident progress report, which may include an updated timeline of the event. The end result of isolation is containment. In the containment phase, the CIRT verifies affected users and systems to ensure only affected systems are contained.

Additional Customer Notifications: Similar to earlier notifications, we may provide Purchasing Entities and third-party stakeholders with available details regarding the incident, possibly including IOCs, containment, and remediation strategy. Purchasing Entities and third-party stakeholders also receive a timeline of events.

Post-Incident Analysis: This stage determines if additional information is available after the initial review of data points documented in the ticketing system and customer notifications. If applicable, we provide newly discovered information about the event. If the new IOCs result in discovering more infected hosts, the process flow returns to kickoff. This stage may be executed in parallel with remediation if all desired forensic information has been captured. The goal is to begin sanitizing systems and re-establishing functional service while performing forensic analysis.

Remediation of Affected Systems: Remediation continues after containment according to the plan developed at the end of the impact assessment. Sanitizing systems usually requires assistance from the incident response team and other ITC division members who work with peer Purchasing Entity response personnel to restore cloud operations. After cleaning affected systems and while restoring service, it may also be necessary to implement measures to prevent further compromise. However, if the revised implementation involves a significant risk (such as temporary loss of availability) or requires a significant level of resources, a plan of action and milestones (POA&M) may be required and revisited later. Recommendations are included in after action reports.

Post Data Breach Notifications: After Action Incident Reports (AAIRs) summarize incident responses for management. If appropriate, Purchasing Entities receive a copy of the AAIR. The recommendations section identifies problems, improvements, lessons learned, and provides a mechanism for vetting those

recommendations. It serves as a place to begin tracking implementation, i.e., a POA&M. The AAIR includes any recommendations that will be placed into incident response procedures, training, or testing exercises. CSRA also provides additional reporting to federal, state, local authorities, and Purchasing Entities. CSRA reports all Advanced Persistent Threat (APT) and national security incidents to the Defense Collaborative Information Sharing Environment (DCISE).

6.3.1.1 Personnel [8.3.1 bullet 1]

Our Contract Manager, Jerome Scherzinger, is the main point of contact for administration, coordination, performance monitoring, and reporting for the MSA. In his role as contract manager, Mr. Scherzinger has full organizational support across the CSRA state and local teams, cloud offering leads, project managers, and human resources, contracts, and legal teams.

Response procedures for potential data breaches include immediately notifying Mr. Scherzinger, who provides initial notification to, and acts as the primary POC for, Purchasing Entities from discovery through incident closure. Depending on the complexity and nature of a potential breach, Mr. Scherzinger coordinates direct communication between CSRA project managers, SOC incident response leads, CSRA IT and communications systems team leads; Amazon and/or Microsoft technical experts; and other subject matter experts as appropriate throughout incident remediation. After incident remediation and closure, he works with the incident response team to develop and provide a comprehensive incident report to the Purchasing Entity.

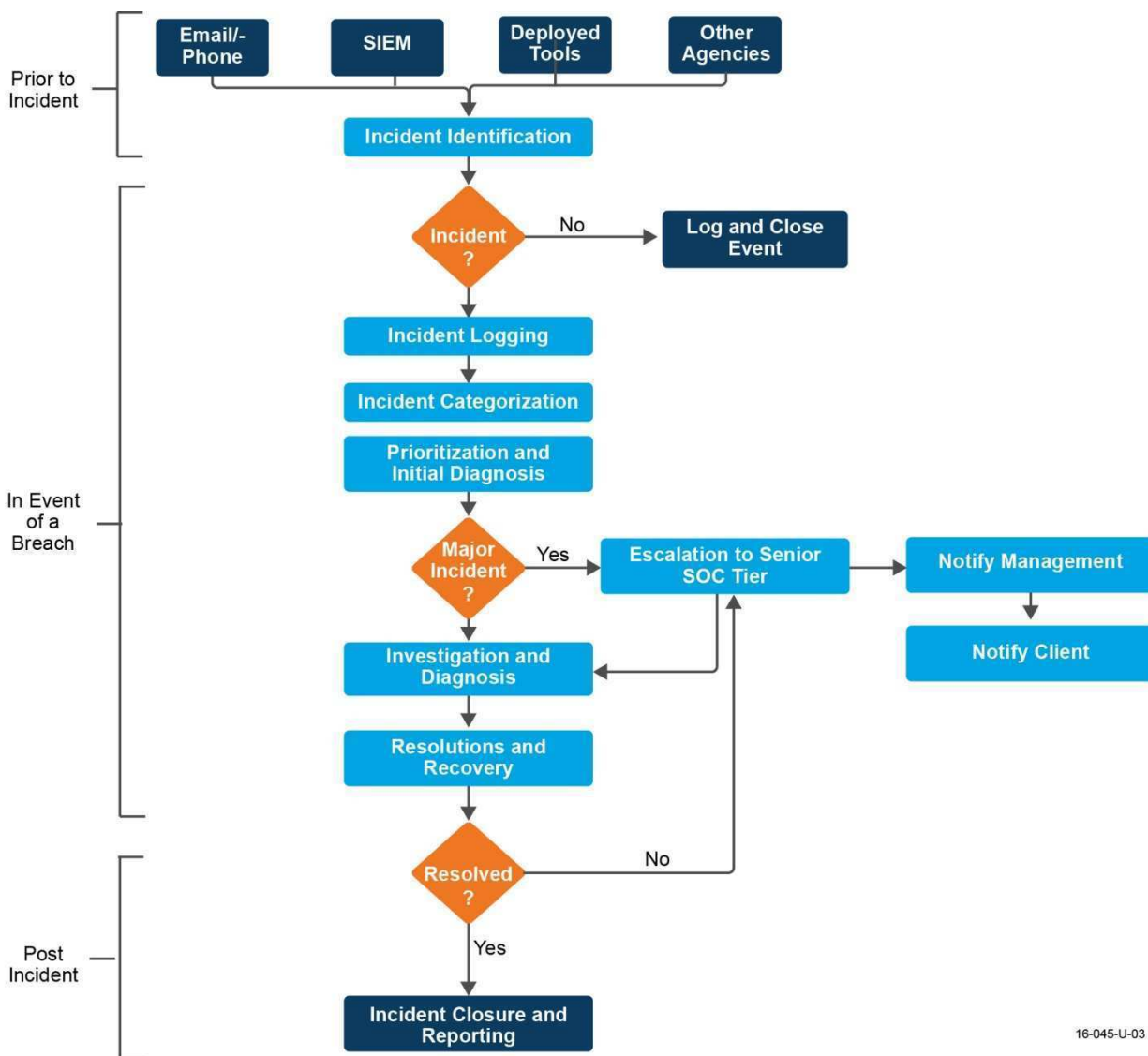
6.3.1.2 Response Times [8.3.1 bullet 2]

CSRA provides an on-premises enterprise security incident response, reporting, and tracking solution for 24x7 security. Our comprehensive, traceable and auditable solution has a central database capable of collecting incident information from inception through resolution.

Cloud Providers: Amazon/Microsoft/Autonomic Incident Management Teams employ industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7 coverage to detect incidents and manage impact and resolution.

6.3.1.3 Processes and Timelines [8.3.1 bullet 3]

The CSRA SOC Focused Operations, SOC Analyst, Engineering, and Compliance Teams comprise the organizational structure behind cyber security operations within the CSRA SOC. These teams ensure the security, resiliency, and reliability of CSRA's IT and communications infrastructure by following defined incident response process in **Exhibit 6-3** over the life of a cyber-incident.



16-045-U-03

Exhibit 6-3. Incident Response Process. Our SOC Incident Management Process ensures the security, resiliency, and reliability of CSRA’s cloud IT and communications infrastructure.

6.3.1.4 Communications and Assistance [8.3.1 bullet 4]

CSRA SOC analysts provide customers with a formal incident reports and classification for the intrusion investigation and incident, ensuring appropriate handling of need-to-know and sensitivity. CSRA SOC analysts work with customer SOC and NOSC personnel and with cloud vendor response personnel. The incident response site lead provides periodic updates to senior CSRA leadership. Senior CSRA management communicates with customers affected by the breach.

Incidents are reported via the incident report form. The Site Lead ensures incident reports identify Who, What, When, Where, Why, and How. Incident summaries are included in the CSRA SOC daily report or other approved rollup reporting. Incident reports are always entered into the ServiceNow ticketing system, the official historical record for troubles of any kind. Any user can contact the help desk to ensure an incident or problem has been reported.

6.3.1.5 Other Information [8.3.1 bullet 5]

All CSRA SOC analysts follow procedures derived from the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01E, Defense in Depth: Information Assurance (IA), and Computer Network Defense (CND).

6.3.2 Certification of not Pushing Adware, Software or Marketing [8.3.2]

CSRA works with the Participating Entity to establish a list of permissions. We work with our vendors to put governance policies in place for activities within our control. As we add new services to our catalog, we work with the service providers to confirm that they abide by these policies. There are matters outside the control of CSRA and its vendors. For example, if a user from a Purchasing Entity uses a browser on a VM in our cloud to visit external Web sites, CSRA cannot control what is pushed to that browser.

6.3.3 Application Hosting and User Test/Staging Environments [8.3.3]

For IaaS and PaaS, CSRA and its vendors do not distinguish among production, test, and development environments. Since we cannot determine the Purchasing Entity's intent for that environment, we treat them all as production. The Purchasing Entity can set up different firewall rules and configuration settings for the different logical environments, but this remains under their control.

Software development and migration services can be provided to the Purchasing Entity for an additional cost. We can design and configure cloud environments to our customers' needs. This includes deploying applications for mission critical systems, protected systems for sensitive data, sandbox development environments or any combination thereof. This excludes SaaS because there is no testing or staging environment. Purchasing Entities who choose to create test accounts in SaaS offerings will be billed as normal accounts.

6.3.4 Compliance with Accessibility Requirements [8.3.4]

CSRA built our portal on ServiceNow, which complies with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794 (d)). In 1998, Congress amended the Rehabilitation Act of 1973 to require federal agencies to make their electronic and information technology accessible to people with disabilities. The law (29 U.S.C. § 794 (d)) applies to all federal agencies when they develop, procure, maintain, or use electronic and IT. Under Section 508, agencies must give disabled employees and members of the public access to information that compares to access available to others. Thereby, applications that comply with Section 508 remain accessible to people with disabilities. In addition to the CSRA portal, the following services also comply with Section 508: ServiceNow, Office 365, Microsoft Dynamics, and the AWS management console.

6.3.5 Web Accessibility Certification [8.3.5]

The supported Web interfaces will change over time as browsers and cloud services evolve. All of our services support released versions of multiple browser platforms. All of CSRA's IaaS, PaaS, and SaaS offerings support the released version of Internet Explorer, Chrome, Firefox and Safari.

6.3.6 Purchasing Entity Meeting [8.3.6]

CSRA will meet with a Purchasing Entity before executing a service level agreement (SLA) to ensure we understand its needs and requirements. Order kickoffs promote collaboration in program execution. Within one week of order award, our contract manager will assign a project manager and conduct a kickoff meeting with government stakeholders. At the kickoff meeting, we begin to build relationships and discuss project-specific roles and responsibilities, schedule, milestones, communications, transition and start-up, resources, and SLAs and metrics. We also will address:

- Type of data stored by Purchasing Entity
- Laws governing data protection
- Intended users of the system
- Mission criticality of the system
- System performance requirement

6.3.7 Project Schedules and Work Plans

CSRA employs a PMBOK-based project management approach to developing project plans, schedules, and work plans. Our process-based approach establishes reliable timelines for development, testing, implementation, and other required tasks. The following processes outline CSRA's management approach to complete projects on schedule:

- Before award the Contract Manager works with the CSRA cloud brand lead and human resources to identify a project manager.
- Upon award, CSRA project manager builds initial work breakdown structure (WBS) and establishes initial development, testing, and implementation schedule using Microsoft Project.
- Project manager meets with delivery teams to review, discuss and modify the WBS as necessary, and to establish accountability for completing tasks and meeting the scheduled dates.
- Project manager completes initial draft of the Project Management Plan (PMP) for review with the Purchasing Entity within 14 calendar days of task award. PMP will be updated to incorporate Purchasing Entity feedback. Resource assignments are finalized and leveled; and task dependencies and milestones adjusted. A final work plan will be submitted within 10 days after receiving Purchasing Entity feedback.
- Upon finalization of WBS and project schedule, the WBS accounts for all project deliverables; all activities are defined and schedule budgets are allocated to each work plan task.
- Throughout delivery, the project manager reviews the status of the plan and updates it as necessary. A project update sheet is generated for Purchasing Entity review and approval
- Throughout delivery, project team members track and record their time, identify when tasks are completed, update estimated hours to complete, identify new tasks that need to be completed, and indicate changes to task end dates. Team members provide weekly progress reports to the project manager, who updates the work plan.
- The project manager reviews the updated plan and the project status at the weekly project team meeting and discusses mitigation approaches to cost and schedule activities. The project manager takes corrective action as needed to keep the project on schedule.

6.4 CUSTOMER SERVICE [8.4]

CSRA's Customer Service Contact Centers (CSCCs) allow organizations in the state and federal space to improve customer service and reduce costs. By leveraging a national infrastructure and the expertise of more than 1,000 CSCC professionals, we deliver enhanced efficiency. Our solution comprises professional personnel and industry-leading processes and technologies, and addresses customers concerns related to:

- Staff and budget constraints
- Lack of predictable costs
- Increased demand for timely response
- Demand for multichannel communication
- Support for social media channels
- Inconsistent customer experience

CSRA's cost effective, multimedia contact center solution provides a single network call queue or multiple call queues. The Call Queue Management Service provides real-time management of routing and distribution of multimedia calls from multiple channels to the call center. CSRA's CSCC services are available for single-site, multiple-site, and enterprise-wide contact centers.

Services Included

- **Attended Service.** Customers communicate in real or near-real time with customer service representatives (CSRs) and social media analysts during normal business hours. CSRA offers attended service over social media, Web chat, SMS/text messaging, phone, and telecommunication device for the deaf (TDD)/teletypewriter (TTY).

- **Unattended Service.** Customers communicate indirectly with CSRs. CSRA offers unattended service over email and postal mail, including customers submitting requests from a website “Contact Us” form and requesting callbacks by phone and from a website “Schedule a Callback” form.
- **Automated Services.** 24x7 automated self-help services. Customers can receive general and account-specific information from our interactive voice response (IVR) system or by browsing our online knowledge base, which includes Frequently Asked Questions (FAQs).
- **Automated Outreach Services.** Mass communications broadcast to targeted customer groups at client’s request. CSRA has the automation capability for completing these campaigns by phone, SMS/text messaging, and email.

CRM Capability Options

Salesforce.com Service Cloud, a FedRAMP certified, commercial off-the-shelf (COTS) CRM suite, selected for its innovative capabilities, rapid, low-risk deployments, out-of-the-box integration with Avaya telephony, and strong third-party plug-in community.

ServiceNow, a platform for inquiry tracking and knowledge management, is augmented by leading tool suites that includes Avaya interactive voice response (IVR), workforce management and actuate reporting.

Telephony Capability Option

Avaya Aura Call Center, this full-service telephony platform coupled with OneSource Networks IVR solution was selected for its reliability, ability to unify the queuing, routing, and automatic assignment of inquiries across all service channels; and available multichannel integration with Salesforce.com or the ServiceNow application.

The CSRA costing model is transaction-based pricing (normally per call or per call band). The pricing model depends on the contract schedules, which vary from fixed unit price, fixed-unit banded price, and time and materials (T&M), but with many similar inputs and drivers.

We offer services in three different tiers structured around performance requirements. CSCCs typically measure the percentage of calls answered within a certain time period, average speed to answer, call abandonment rate expressed as a percentage of total calls, percentage of emails responded to within a specified time, customer satisfaction levels, and service availability. Performance can be modified to provide higher or lower levels of service with a corresponding increase or decrease in the associated pricing for the different tiers. **Exhibit 6-4** shows an example of performance standards, Acceptable Quality Levels (AQLs), and disincentives for time to answer calls in Gold, Silver and Bronze tiers for the single requirement for percentage (85%, 75%, 60%) of calls answered within a specified time period (30 seconds, 60 seconds, 120 seconds).

Performance Requirement/Service Level	Performance Standard	Method of Measurement	AQL	Method of Surveillance	Disincentive
Gold (telephone inquiries)	Percentage of calls answered within 30 seconds or less	Monthly average based on individual programs	85% or more of calls handled	Statistics gathered from ACD system	If monthly average shows less than 85% of calls answered within 30 seconds, a 1% disincentive is deducted from the monthly invoice
Silver (telephone inquiries)	Percentage of calls answered within 60 seconds or less	Monthly average based on aggregate contract level performance	75% or more of calls handled	Statistics gathered from ACD system	If monthly average shows less than 75% of calls answered within 60 seconds, a 1% disincentive is deducted from the monthly invoice

Performance Requirement/ Service Level	Performance Standard	Method of Measurement	AQL	Method of Surveillance	Disincentive
Bronze (telephone inquiries)	Percentage of calls answered within 120 seconds or less	Monthly average based on aggregate contract level performance	60% or more of calls handled	Statistics gathered from ACD system	If monthly average shows less than 60% of calls answered within 120 seconds, a 1% disincentive is deducted from the monthly invoice

Exhibit 6-4. Example of Pricing Based on Service Tiers. Gold, Silver, and Bronze service levels

6.4.1 How Purchasing Entities Provide Customer Service [8.4.1]

CSCCs may be used in conjunction with Toll Free and other network services to facilitate communications with the general public, businesses, and other agencies. Along with the Call Queue Management Service, CSCCs provide a Call Answering Service that enables customers to use CSRA-provided resources to respond to caller inquiries. The call answering resources can be situated at either Purchasing Entity or CSRA locations.

CSRA's CSCCs interoperate with the Internet and Public Switched Telephone Network (PSTN) using underlying network services and their interfaces to deliver customer service capabilities. CSCCs may be ordered as a domestic (CONUS) or nondomestic (OCONUS) service. The majority of CSRA's support platforms reside in CONUS and the geographical scope for the local, national, and international coverage will vary with CSRA's network.

CSRA allows customers to choose the delivery channel best suited to them. We will work with Purchasing Entities on call flow design, development, and maintenance of the information and audio messages used for all automated voice response services (e.g., IVR, voice recognition, and text-to-speech). With any channel, our solution enables Purchasing Entities to track, respond, and report on the 360-degree view of each customer experience. CSRA's technology solution optimizes all aspects of the CSCC as shown in [Exhibit 6-5](#).

Function/ Feature	CSRA Proposed Technology Solution	Strengths
Customer Relationship Management (CRM) solution	Regardless of access channel, CRM system tracks inquiries from initial contact through resolution while maintaining and displaying the 360-degree historical view of customer's experience.	Agents address each request with sensitivity to entire customer experience.
Call Processing	- IVR greets callers and, after verification, provides 24x7 access to self-service options. - IVR services provided in English and Spanish using natural language processing and speech recognition. - Callers requesting live assistance are routed to CSRA's Geo-Redundant IVR. The IVR captures the caller's Automatic Number Identification (ANI) and queries the CRM to retrieve and pass the caller's contact record's associated application Uniform Resource Locator (URL) and ANI and IVR departure point code to the telephony system.	Consistent handling of inquiries from all channels.
Queuing	Universal work queue holds calls, emails, chat sessions, texts, and all other channel inquiries, informing callers and chat contacts of expected wait time (EWT) and reminding them of available self-service options.	Single queuing provides CSRA and customer a view into the entire customer experience, including historical and frequency information.

Function/ Feature	CSRA Proposed Technology Solution	Strengths
Automated Voice Response	On Site Notification (OSN) IVR provides voice user interface for voice recognition programmed with relevant terms, supports Speech Synthesis Markup Language (SSML)/Voice Extensible Markup Language (XML), and provides speech recognition, dynamic language detection, voice authentication, dynamic grammar, natural language, partial phrase recognition, and caller interrupt features.	Increased customer self-help and reduced need for attended support.
Computer Telephony Integration	CSRA's multichannel telephony solution provides data-driven screen pop-ups, a unified agent desktop, a universal work queue for all channels, and blended inbound and outbound communications.	Optimize productivity and CSRs' ability to view all relevant information on their desktops.
Text Messaging	Text messages received by our platform, which places the incoming Short Message Service (SMS) into our universal work queue and routes it to next available CSR.	This interactive platform is particularly useful for customers who rely on texting for communications.
Telecommunication Device for the Deaf (TDD)/ Text Telephone (TTY)	If an agent is not immediately available, CSRA's solution under specific circumstances and based on advanced algorithms that calculate EWTs, provides EWT informational messages in native TDD/TTY tones.	Callers with special needs receive the same level of service as other inquirers.
Postal mail routing and management	Postal mail will be routed through the CSRA BPO center, where letters will be opened, recorded, scanned, and uploaded into the CRM for adjudication.	Postal mail is turned into electronic case material and processed the same way as other correspondence.
Knowledge Management System	CSRA configures an integrated knowledge management (KM) system in CRM for storing, organizing, searching, and retrieving the information necessary to respond to contact inquiries.	Continuously updated KM system enables CSRs to resolve inquiries quickly and feed FAQs.
Workforce Management	CSRA Workforce Optimization system is used by supervisors to create employee schedules based on call volume from previous days, weeks, months, and even years.	Ability to proactively respond to fluctuations in contact volumes.
FAQ System	The CRM Knowledge Management System publishes e-knowledge articles and FAQs on customer's web site via an embedded link to a CRM-hosted site.	Continually updated FAQ articles answer questions, thus reducing calls to the contact center.
Publication Ordering System	Publication orders are processed as a case in the CRM. The adjudicated request is routed to the mailroom for production.	Eliminates the need for a separate tracking and reporting system for publication ordering.
Customer Survey Automation	CSRA integrates customer satisfaction surveys into the Customer Feedback System and enables service recovery opportunities through alerts.	Automated routing reduces handling time and opportunity for manual variances.
Customer Satisfaction and Complaint Management	Customers can submit compliments, complaints, suggestions, and comments via voicemail from an ACD option using our Asterisk voicemail via an electronic form on the hosted Web page or email.	CSRA monitors customer satisfaction and implements Process Improvement Plans as needed.
Service Monitoring and Quality Control (QC)	Web-based Workforce Optimization modules monitor customer interaction with contact centers, along with CSRA's Quality Assurance (QA) Management Guide and in-house QC process.	Service levels are maintained.

Function/ Feature	CSRA Proposed Technology Solution	Strengths
Fulfillment System	- Orders processed as a case in the CRM. - Adjudicated requests routed to appropriate resources for production.	Single tracking and reporting system for fulfillments.
Dialed Number ID Services	ACD solution can use dialed number ID services.	Agents can use this information to route calls.
Call Transfer	- ACD routes call based on predetermined criteria to specific groups in CSRA's contact center operations. - Ability to transfer callers based on their selection in the IVR to specific department or persons.	CSRA telephony system records and reports on transferred calls along with all other inquiry information.

Exhibit 6-5. CSRA's Innovative Technology Solution. *CSRA's proposed functions, features, and strengths.*

6.4.1.1 Quality Assurance Measures [8.4.1 bullet 1]

CSRA's Quality Control Plan (QCP) provides a framework of processes and procedures based on our QualityFirst program. We customize the framework for each Purchasing Entity's environment and focus on delivery of service and process improvement initiatives, which ultimately results in high customer satisfaction. Our multifaceted total quality management approach includes benchmarking industry standards, executing best practices, and evaluating performance and processes for continuous improvement.

Our comprehensive monitoring approach includes sharing responsibility for enhancing the quality of CSCC operations and CSR performance development across QC, operations, project and content management, and training. Representatives from each of these CSRA entities share the responsibility for enhancing the quality of Customer Service Contact Center operations and for assisting in CSR performance development. All monitoring personnel receive training from the QA team on the QC monitoring program and processes before monitoring, and participate in mandatory monthly QA sessions.

CSRA concentrates on delivering superior customer support and high quality of service (QoS). An integrated customer inquiry tracking functionality, which authorized on-site and remote users can access, supports all contacts made to the CSCC. ServiceNow captures records and tracks all relevant data. After a call has been routed, the CSR looks up the customer to classify the call as a repeat or new inquiry. The application flow supports the selection of an existing or new SR.

The system tracks various types of data demographics for inquiry disposition, including capture and retention of program-specific data such as case (i.e., SR) number, caller name, applicant name, date/time of contact, disposition code, QC analysis, inquiry status/type, associated program, methods of inquiry receipt/response, follow-up assignments and related transfers/escalations; follow-up and closure details; FAQs, and the ability to link duplicate inquiries to support call flow. Whether the customer contact is new or a repeat inquiry, ServiceNow supports the CSR in establishing activity records for inquiries that require follow-up, escalation or callback.

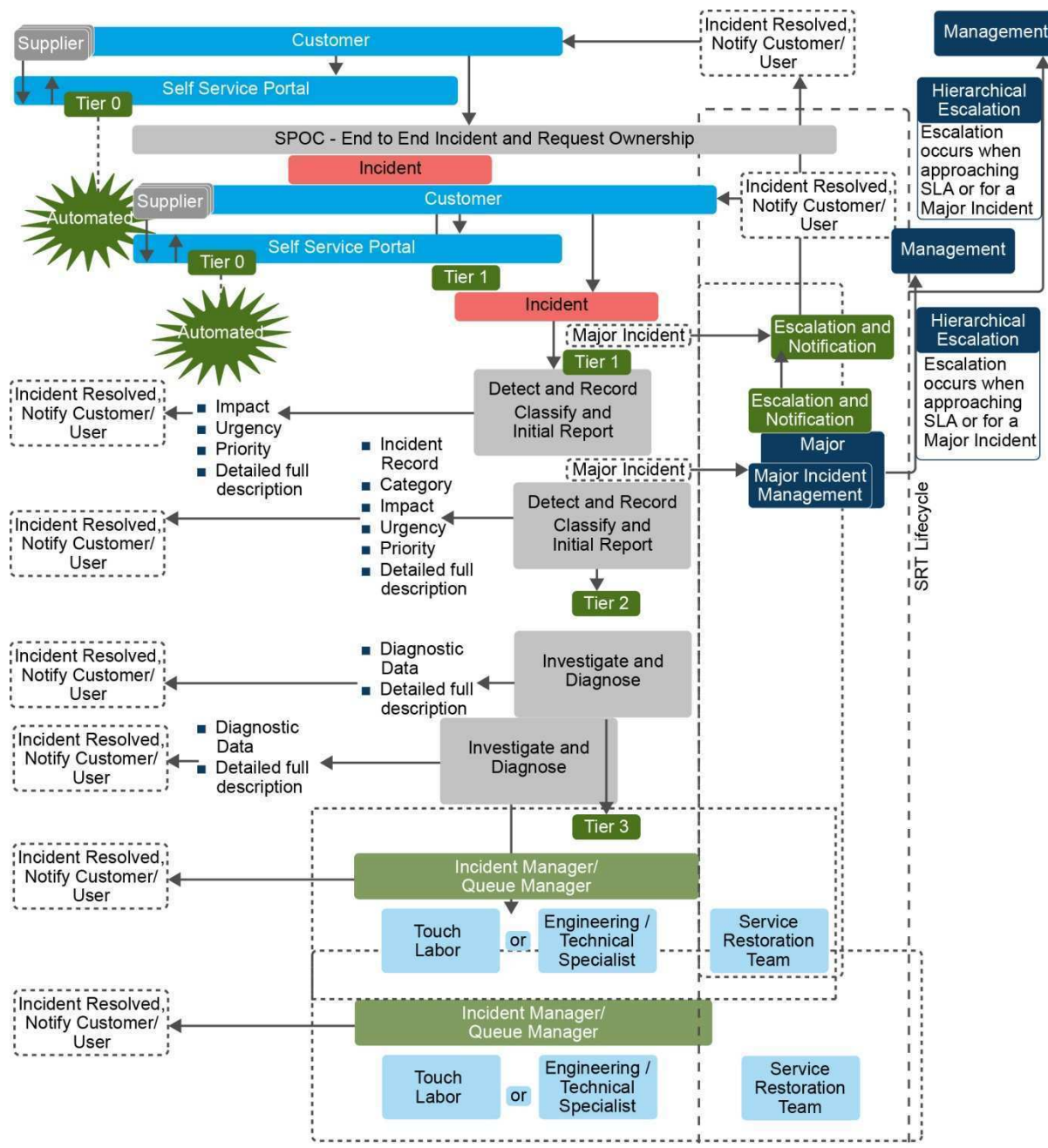
Through the services defined in this solution, the Purchasing Entity realizes the following objectives:

- CSCC services meet or exceed private industry standards by providing accessible, accurate, and timely responses to customer inquiries via their preferred communication channel.
- Capability to provide managed multichannel inquiry response and management solutions that meet customer needs.
- Operational readiness to manage contact center volume fluctuations while performing within SLA targets.
- Flexibility to add programs, Contact Centers, and customized services as required. Programs may include internal, external (from other agencies) or private industry customers.

- Increased capability to measure and control delivery of information services to meet citizens' needs; and provide centralized delivery to better control and improve customer satisfaction.
- Gain and sustain access to secure and scalable COTS technology to meet requirements.

6.4.1.2 Problem/Complaint Escalation Plan [8.4.1 bullet 2]

The CSCC escalates issues and provides solutions as shown in **Exhibit 6-6**. The CSCC Program Management Office (PMO) coordinates with other PMOs, system vendors, and stakeholders.



16-045-UT-08

Exhibit 6-6. Escalation and Notification. Customer Service Contact Center delivers end-to-end incident and service request ownership and accountability.

Customer Complaint (Customer Complaint Record)

A Customer Complaint Record documents complaints of unsatisfactory performance, the time and date the customer notified the responsible official, the validity of the complaint, and corrective actions. When a complaint is received, the Purchasing Entity completes appropriate documentation to record the complaint on a surveillance form. CSRA works with customers to develop standard surveillance forms if none exist. The Purchasing Entity verbally notifies and emails the CSRA quality manager the complaint. The quality manager typically has 24 hours after verbal notification to implement corrective action. After site investigation, the quality manager notifies the Purchasing Entity if they challenge the validity of the complaint. The Purchasing Entity conducts its own investigation. If they determine the complaint is invalid, the findings are documented and the customer notified. The Purchasing Entity retains the annotated copy of the written complaint. If the Purchasing Entity determines the complaint is valid, the Purchasing Entity informs the quality manager, who typically has an additional 24 hours to implement the correction. The total number of customer complaints received is documented on the surveillance form.

6.4.1.3 Service Level Agreements [8.4.1 bullet 3]

CSRA has more than 15 years of experience planning, implementing, and meeting performance measures for call and contact centers. For contracts that measure key performance indicators, we consistently exceed performance levels. Our standard performance measures include service levels, average speed to answer, abandonment rate, first-call resolution, average handle time, CSR occupancy, shrinkage, schedule adherence, internal quality measures, and external quality measures using a third-party evaluator.

Our standard service delivery model for customer service support operations includes reporting incident and service management statistics and performance. CSRA employs advanced service management and reporting tools for standard and *ad hoc* reporting and to facilitate publishing content for CSRA and client use.

CSRA collects metrics from multiple sources in order to evaluate and understand volumes and performance. These metrics, or key performance indicators (KPIs), differ from SLAs because they are informational rather than contractual. Customer service support uses metrics for real time management and stores them for reporting purposes. CSRA collects data from the ACD, including the number of inbound calls, abandon rate, number of voicemail calls, and the average speed of answer. Customer service support tools provide CSRA with data that includes the number of requests handled, number of incidents opened, number of incidents resolved, percent of tickets resolved, and the time to resolve. Customer service and clients use this data to assess productivity and evaluate services. For example, every week our customer service examines the top 10 problems for each client, and uses this data to initiate an RCA, update the knowledge base or add a FAQ to the portal.

We provide the standard Gold level SLA below as an example. The CSRA CSCC offers Purchasing Entities additional options (Silver and Bronze) for lower SLA targets as a tradeoff for lower costs. The Purchasing Entity may ultimately establish different service levels for the contract performance standard and substitute them in place of the example.

- Work Area:
 - Operational Performance
 - 85% of phone calls answered within ≤ 30 seconds; average speed to answer ≤ 30 seconds; abandoned rate of $\leq 5\%$
 - Voicemail
 - Outbound Calling Service
 - Management Reports
 - Customer Satisfaction Survey

CSRA uses the following best practices and KPIs as guidelines in the IT service desk industry.

- Daily service reviews and continual service improvement initiatives

- Planning and execution of training opportunities
- Maintain change management controls within the environment

Key Performance Indicators

- Average speed to answer (ASA) – typically within 30-60 seconds
- First Call Resolution (FCR) for resolvable calls only –the percentage resolved on first contact. Typically contact centers aim for $\geq 75\%$ to 95% FCR rate
- Call abandonment rate – targets are usually set at $\leq 5\%$ of all incoming calls.
- Customer Satisfaction rating – this survey uses a scale of 1 to 5, with 5 as the highest (the industry standard is ≥ 3.5)

Based on Purchasing Entity requirements, we evaluate customer satisfaction as part of the customer service solution. CSRA recommends a standard customer satisfaction survey or collaborates with the Purchasing Entity to tailor the program. We can automate polling, collection, tabulation, and reporting of customer satisfaction surveys and their results. Customer satisfaction reporting can include recommendations to improve processes, procedures, and tools.

CSRA works with Purchasing Entities to determine the most appropriate means to communicate service levels and performance metrics. Reports can be delivered via a customer portal and presented at client service delivery meetings. CSRA also offers an optional service to integrate dashboards into the customer service tool set for clients seeking visibility and on-demand access to service information.

6.4.2 Compliance with Customer Service Requirements [8.4.2]

CSRA provides all planning, design, implementation, operation, compliance, maintenance, and management of technology supporting CSCC. Specialized software monitors all systems. It can detect if a particular component experiences an issue. CSCC staff has desktop technology to support access to all solution systems and components, inclusive of telecommunications, email, and Internet access.

The Web-based ServiceNow application allows CSRs to research information in the local knowledge base or external resources to answer customer inquiries. ServiceNow identifies government-approved sources and helps CSRs select the right resource based on information provided by the caller. The scripts serve as guides for call handling. **Exhibit 6-7** details our customer service capabilities.

Element	Description
Call Routing and Distribution	The Avaya Automated Call Distribution (ACD) system routes calls from the PSTN to available CSRs based on availability, assigned skills, and other predefined routing instructions. Supervisors and site managers use the Call Management System to monitor and display real-time work state and availability of CSRs. It can also display call-handling statistics in real time and provide the ability to save or print reports on all trunks, CSR, and workgroup performance statistics.
Automated Voice Response (AVR)	CSRA's proposed AVR/ IVR system uses effective voice response solutions that enable callers to locate answers to FAQs in a customer-friendly manner. The system differentiates between calls made during business and nonbusiness hours, with the ability to report on callers' selections by menu.
Call Queuing	The ACD system transfers incoming calls to a dedicated queue and plays a message advising callers of estimated wait time and position in queue, or can play alternative recorded messages as required. The ACD allows callers to choose to stay in the queue or to leave a message for a callback by using prompts from the ACD menu.
Inquiry Management	The focal point of our solution, the ServiceNow cloud software, supports the bulk of the government's core contact center requirements, thus requiring minimal customization. ServiceNow complies with all Section 508 requirements, and CSRA ensures all other applications are accessible as required by Section 508. This scalable cloud-based solution easily handles fluctuations in inquiry volume, and offers the highest level of availability. CSRA provides the inquiry processing technology and services required to handle the workload the CSCC presents.

Element	Description
Inquiry Tracking	ServiceNow records and tracks all relevant data related to inquiries. The core of the system is the SR record on which all inquiry data is recorded and response details are associated. From the SR record, system users can review all aspects of an inquiry. SRs are time stamped when opened and closed in support of SLAs. SRs are assigned to a representative for processing and show within the representative's "to-do" list until complete. SRs are searchable and updatable, and all relevant data is available for reporting.
Accounting and Management	ServiceNow categorizes and tracks all inquiry types. It tracks details such as contact source, program, language, and inquiry categorization in the SR record. All relevant data is available for reporting.
Email Routing and Management	ServiceNow's configurable email solution provides efficient ingestion, pre-processing, assignment, and response. It can be configured to automatically extract data from electronic inquiries for population into corresponding database fields.
Knowledge Management (KM) System	CSRA uses ServiceNow to configure an integrated KM system for storing, organizing, searching, and retrieving information necessary to respond to contact inquiries. ServiceNow's Web interface to knowledge content provides an easy-to-use method for posting, updating, searching, and retrieving information. Representatives can provide knowledge content directly to callers or include it in email or Web chat sessions. The system creates a tracking record on the SR of knowledge content used to support an inquiry, allowing customers to report the frequency of use of knowledge content.
Contact Management (CM) System	CSRA's case management methodology facilitates tracking a contact's inquiries from initial contact through resolution, regardless of the access channel used. A contact (customer) might have one or more SRs related to their inquiry history. The SRs identify the information the customer received from the contact center or portal, and any information the customer provided. Blended channel communications are captured within a single SR as separate activity records. CSRA provides summary, and systems and management data via secure Web access.
Work Force Management (WFM) System	CSRA deploys the Avaya Work Force Optimization (WFO) system to forecast, manage, and schedule all contact center activities. Base agent schedules are built on forecasted demand and arrival patterns then optimized to include all off-phone activities such as breaks, team meetings, coaching sessions, and refresher training. The WFM team chooses the best schedule based on call volume, desired work pattern of the employee, projected service level, and average talk time of past calls. Our WFM team manages employee schedules, optimizes to achieve performance expectations, and coordinates with the program and site managers to communicate any identified variance from established planning. Through Avaya WFO, we can schedule associates and audit adherence to the schedules to ensure client service levels are achieved. If a change in the associate schedule is required to meet customer needs, WFM can adjust the associate's schedule in real time, and the system alerts the impacted associates via a desktop notification that a change has been made to their schedule. In this way, WFM can manage and optimize a multisite workforce as one virtual collection of resources in an efficient fashion regardless of the agent's location. The WFO system also empowers our WFM team, managers, supervisors, and agents to work from the same information, because all users have access to the system. Based on user role, individuals can see their, the group's or CSCC performance on the scorecards module of the platform. This capability allows each individual to see the metrics they are responsible for or the impact in relation to the goal established for that metric. Additionally, trending information is available to highlight whether their performance improves or holds at prescribed goal levels. Our WFM and operations teams also leverage the Call Management System to set skill and agent-level routing priorities. This capability allows for the ability to have specialized agents on specific programs while serving as backup or reserve agents for other programs. Through this strategy, agents can hone their skills on individual programs, and as their skills grow, additional programs are added to their routing to enable a flexible workforce.

Element	Description
Customer Survey Automation	CSRA integrates customer satisfaction surveys into the IVR in accordance with rules prescribed by customers. Our IVR system records answers to survey questions and provides the means to sort, aggregate, and report survey results.
Customer Satisfaction and Complaint Management	Customers have the ability to submit compliments, complaints, suggestions, and comments via voicemail from an ACD option via our Avaya Audix LX voicemail system, an electronic form on the hosted Web page or email. CSRA transcribes and capture all submissions in a central location for analysis.
Service Monitoring and Quality Control	CSRA uses a QA Web application for monitoring customer contacts. We developed the application in conjunction with its QA management guide and in-house QC process. The CSR application allows recording and storage of contact monitoring forms and is used to produce QA reports.
Training	Each of CSRA's contact centers has training facilities for on-site training classes. Each facility is configured with trainee workstations loaded with the software to support the training class and a projection system used for multimedia presentations and demonstrations.
Voicemail and Email	CSRA uses the Avaya Intuity Audix LX voicemail system to provide voice mailboxes where customers can leave messages with suggestions, comments, and call-back information. Voicemail services are integrated and accessible from all components of CSRA's telephony infrastructure and are sized to handle surges. CSRA maintains a duplicate hot standby Intuity Audix LX voicemail system for disaster recovery (DR), which can also be used for surges if necessary. CSRA maintains secure offline storage of voicemails for 90 days from the record date stored in .wav format.

Exhibit 6-7. CSRA's Technology Solutions. *CSRA's compliance with customer service requirements*

6.4.2.1 Lead Representative for Each Entity [8.4.2 (a)]

A CSRA **project manager** is assigned for each task order as the lead representative for each entity throughout execution. The project manager's contact information will be kept current and maintained for record by the Contract Manager. The project manager is responsible for individual task requirements: organizes, directs, coordinates planning, and implements all project support activities; interacts with program officials regarding issues and status of the project; coordinates financial and staffing resources; monitors and analyzes performance data and reports results to the government; coordinates training activities to keep staff current on programs and customer service objectives; manages the activities of subcontractors; and prepares operations and management reports.

6.4.2.2 Availability of Customer Service Representatives [8.4.2 (b)]

CSCC hours of operation are Monday through Sunday, 7:00 a.m. to 6:00 p.m. in each applicable time zone CSRs are available via phone or email during the hours of operation. CSRA offers options to standard operating hours, including 24x7 support for programs requiring greater coverage. Round-the-clock contact center operations require experience in forecasting and scheduling as well as a flexible workforce. We recruit and train staff with the knowledge that their schedules and duties may change. This flexibility allows us to adapt to unexpected situations that affect call volume and workforce availability.

For programs requiring less coverage or reduced costs, CSRA offers CSCC services between 7:00 a.m. and 6:00 p.m. in each applicable time zone, Monday through Friday, excluding negotiated holidays. CSRA can expand or reduce hours of operation for customer service support as required, including adding coverage for weekends, evenings, and federal holidays. We use this option for special events or as a longer-term alternative to 24x7 support.

CSRA can provide 24x7 support, augmenting staff for short-term and long-term surges, and ramping up to meet priority requirements. Our facilities have available additional capacity in the form of ready workstation areas and empty space for build out. We can begin facility, technology, and staffing ramp up within one hour of notification.

To accommodate unforeseen demand increases in contact center operations, CSRA leverages cross-trained CSRs to provide backup support. CSRA's staffing can accommodate surges of 10 percent or less of the daily forecasted volume without affecting service levels. With 48 hours' notice, we can increase staffing by an additional 10 percent through the use of overtime and leveraging pre-trained, nonproduction resources such as QA analysts, trainers and operations managers to meet short-term increased demand capacity. If we receive at least 21 days' notice of an upcoming surge we can add CSRs to increase capacity in large quantities, limited only by the ability to hire qualified candidates and attain the appropriate clearances to support the customer program. We provide affordable, flexible approaches to address unanticipated call volume needs.

6.4.2.3 Customer Service Representative Response Time [8.4.2 (c)]

CSR response time is one business day. First-contact resolution is an important driver of customer satisfaction and CSCC efficiency, and we encourage and incentivize first-contact resolution. We capture and track information related to inbound inquiries and outbound interactions, such as the date and time of contact receipt, nature of inquiry, source of inquiry, and information requested. CSRA offers automated responses, telephone response, TDD/TYY response, electronic response, post mail response, facsimile response, form letter response, interim response, coordinated response, and referrals.

Our real-time interactions during attended services (phone and Web chat) may spawn requests for information sent by other means such as email, mail or SMS/text message. Our CSRs fulfill all requests accordingly.

If after evaluating and responding to unattended inquiries such as an email, the CSR requires additional information, they reach out to the customer through a contact channel. If further research will delay response, we provide an interim response that informs the customer of when we estimate we can provide a complete response. If a coordinated response is required for issues involving legal matters, policy interpretation, or a technical response that cannot be answered readily from the knowledge base, we refer the issue to the appropriate authority for direct response. CSRA collects information from the inquirer to give the appropriate authority enough detail to enable a timely response.

CSRA re-directs or refers misdirected inquiries, out-of-scope inquiries, and inquiries that require information from a different entity to the appropriate organizations identified in the referral list in our knowledge base. CSRA staff analyzes inquiries, assess response modes, gather information from customer-approved sources, confirm the information's accuracy, and provide information or assistance via the inquirer's preferred communication medium. Performance requirements and standards are shown in **Exhibit 6-8**.

Performance Requirement	Performance Standard	Method of Measurement	AQL	Method of Surveillance
Service Level (telephone)	Percentage of calls answered in ≤ 30 seconds	Monthly average	85%	Statistics gathered from the ACD system
Average Speed of Answer	Total seconds to answer divided by number of calls answered	Monthly average	≤ 30 seconds	Statistics gathered from the ACD system
Abandonment Rate	Percentage of calls dropped or hung up prior to accessing a live CSR	Monthly average	≤ 5%	Statistics gathered from the ACD system
Email Response Time	Percentage of emails responded to within 1 to 2 business days	Monthly average	98% within 1 business day; 100% within 2 business days	Statistics gathered from the ServiceNow platform
Customer Satisfaction	Percentage of callers indicating satisfaction as ≥ 3 on 5-point overall customer satisfaction	Monthly average	90%	Statistics gathered from the ACD system

Performance Requirement	Performance Standard	Method of Measurement	AQL	Method of Surveillance
	survey			
Service Availability	Percentage of time that service is available as defined in the contract	Monthly average	99.9%	Statistics gathered from the ACD system

Exhibit 6-8. CSRA Performance Metrics. *CSRA's performance requirements and standards*

6.4.2.4 Design Services [8.4.2 (d)]

CSRA's discovery and design services are offered at a fixed cost to the Purchasing Entity as part of our cloud migration services. A cloud architect works with the Purchasing Entity to include all its requirements in the design. Purchasing Entities can acquire the design services or the full migration of its environment. Our catalog's range of design service offerings can be tailored to meet specific Purchasing Entities' needs.

6.4.2.5 Installation Services [8.4.2 (e)]

CSRA offers installation services for all of the categories in our solution. Purchasing Entities can use our cloud migration services to get their applications into the cloud. Our modernization and migration process reflects industry-best practices. Our core processes, artifacts, and decision criteria drive all migration planning and execution activities across Physical-to-Physical (P2P), Physical to Virtual (P2V) and Virtual to Cloud (V2C) migrations. These processes have been used successfully on government migrations, including for the Center for Medicare and Medicaid Services (CMS) Development Environment Consolidation Contract (DECC), where we moved more than 200 legacy systems to a new target environment on schedule and under budget. We have refined our process so that we can offer this service as a fixed price option, allowing our customers to always know the cost of migrating to the cloud. Most other service providers charge by the hour for migration services, with no guarantee of final cost.

6.5 SECURITY OF INFORMATION [8.5]

Data Protection Measures

Purchasing Entities retain control and ownership of their data and all data the cloud vendors' store. Each CSP has tenant isolation security and control capabilities implemented on behalf of their customers. Purchasing Entities should consider their data sensitivity requirements for data in transit at rest.

Cloud providers offer the following secure technologies to ensure availability, integrity and confidentiality of Purchasing Entity's data.

6.5.1 Data Protection [8.5.1]

Data at Rest

Options for encrypting data at rest range from completely automated vendor encryption solutions to API-coded or manual, client-side options. Choosing the right solutions depends on the cloud services used and customer requirements for encryption and key management. When considering encryption, Purchasing Entities have two primary choices:

1. Encrypt the underlying storage so all data is automatically encrypted
2. Encrypt each piece of data as it is stored

From a usability perspective, reducing the need to worry about encryption for daily operations is optimal. This usually leads to the encryption of the underlying storage. Encryption choices are:

Security of Information

- CSPs provide confidentiality, integrity, and availability of customer data
- Customers inherit all the best practices of CSP policies, architecture, and operational processes
- CSRA and the CSP's offer tools and features to help meet security objectives around visibility, auditability, controllability and agility
- CSP environments are audited with certifications from accreditation bodies across geographies and verticals

- **AWS:** Amazon automatically encrypts data at the object level as it writes to disks in its data centers and decrypts it on access. AWS uses AES 128 and 256 bit encoding for default encryption and for customers with FIPS 140-2 requirements, SSL terminations in AWS GovCloud (US) operate using FIPS 140-2 validated cryptographic modules.
- **AWS Key Management:** AWS' key management service (KMS) provides centralized control of encryption keys. KMS presents a single view into all of the key usage by an organization. Purchasing Entities can create keys, implement key rotation, create usage policies, and enable logging from the AWS Management Console or use an API.
- **Microsoft Azure:** Microsoft Cloud offers a range of encryption capabilities from AES 128 bit up to AES-256, giving Purchasing Entities flexibility to choose the solution that best meets their needs. FIPS 140-2 data encryption is available from the BitLocker FIPS-compliant environment.
- **Microsoft Azure Key Management:** Azure Key Vault (AKV) helps safeguard cryptographic keys and secrets used by cloud applications and services. By using AKV, Purchasing Entities can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys protected by hardware security modules (HSMs). For added assurance, Purchasing Entities can import or generate keys in HSMs. If an Entity chooses to do this, Microsoft will process the keys in FIPS 140-2 Level 2 validated HSMs (hardware and firmware).
- **ARC-P:** ARC-P does not provide disk encryption services.
- **ARC-P Key Management:** ARC-P exposes the Intel AES-NI instruction set within instances to facilitate disk encryption with the guest OS of the instance. (Microsoft BitLocker, Linux dm-crypt/LUKS or equivalent software).

Data in Transit

- Protecting data in transit involves protecting network traffic between clients and servers or network traffic among servers. Cloud provider services support Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. Purchasing Entities hosting a Web server in an IaaS, SaaS or PaaS instance assume responsibility for data in transit encryption. SSL/TLS is used for any HTTP traffic with a validated certificate from a trusted third party. If the deployment does not use HTTPS as a transport, the encrypted equivalent for the protocol used must be found. It is important to note that there is little performance impact on an all-encrypted communications channel.
- **AWS** protects data in transit with support for SSL/TLS in CloudFront, Amazon RDS, and elastic load balancing.
- **Microsoft Azure** uses industry-standard secure transport protocols such as IPsec and SSL/TLS between user devices and Microsoft data centers, and within data centers. Azure Virtual Networks allow use of the industry-standard IPsec protocol to encrypt traffic between corporate VPN gateways and Azure or among VMs located on Purchasing Entities' Azure Virtual Networks. Microsoft Office 365 and other offered services follow industry cryptographic standards such as SSL/TLS and AES to protect the confidentiality and integrity of Purchasing Entity data.
- **ARC-P** uses the ARC-P SecureGateway with multi-factor authentication (MFA), a FIPS 140-2 Level 2 validated device, for orchestration of cloud resources. With ARC-P Virtual Private Cloud (VPC) Purchasing Entities can use the IPsec protocol to encrypt traffic between physical networks and virtual networks hosted in the cloud.

Data Disposal

CSRA promotes understanding of the following data ownership and management fundamentals in the cloud shared responsibility model. Purchasing Entities:

1. Own their data.
2. Choose the geographic locations where to store their data—it does not move unless the Entity decides to move it.
3. Download or delete their data whenever they like.

4. Consider their data sensitivity requirements for data in transit at rest.

Our cloud vendors commit to the privacy of Purchasing Entity data and backed adoption of international code of practices for cloud privacy, ISO/IEC 27018. Third-party auditors independently verified enterprise cloud providers to ensure they align with the ISO 27018 code of practice for the protection of personally identifiable information in the public cloud. Adherence also ensures transparency about the return, transfer, and deletion of personal information stored in vendor data centers. Details include:

AWS: Purchasing Entities have the ability to delete their data. AWS customers retain control, ownership, and management of their data.

AWS Storage Device Decommissioning: When a storage device reaches the end of its useful life, AWS procedures include a decommissioning process designed to prevent customer data from exposure to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Microsoft Azure: Data destruction techniques vary depending on the type of data object, whether it is a whole subscriptions, storage, VMs, or databases.

- **Subscriptions:** If a purchased subscription (like Office 365) has expired or is terminated, all associated customer data is held for 90 days before it is deleted to recover from accidental subscription cancellation. In no more than 180 days after expiration or termination, Microsoft disables the account and deletes customer data. Storage accounts terminated within an existing subscription (or when a subscription deletion has reached its timeout) are not deleted for an additional two weeks to prevent mistakes.
- **Storage:** Once a storage account is deleted or when blob or table data is deleted outside the context of a storage account deletion, the disk sectors are immediately available for reuse. How long before they are overwritten depends on the fullness and activity rate on the server, but is rarely more than two days.
- **Virtual Machines:** Virtual machines are stored in Microsoft Azure Storage as blobs, so the deletion rules apply as explained above in Storage. The virtualization mechanism ensures that another customer cannot read the spot on the disk until the data gets written again, thus mitigating the threat of data leakage. When a new virtual disk is created for a VM, it will appear to the VM to be zeroed, however, the explicit zeroing of the data buffers occur when a portion of the virtual disk is read before it is written. If a VM instance is reinitialized in place, it’s the same as if it had moved to new hardware.
- **Azure SQL Storage:** Azure SQL Database deleted data is marked for deletion. If an entire database is deleted, it is the equivalent of deleting the database’s entire contents. The SQL Database implementation ensures that user data never leaks by disallowing all access to the underlying storage except via the SQL Database API.

Microsoft Azure Storage Device Decommissioning: When a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before Microsoft returns it to the manufacturer for replacement or repair. All of the data on the drive is completely overwritten to ensure that the data cannot be recovered. When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

ARC-P: All data within the Purchasing Entity’s VM remains under the Entity’s control. It is the Entity’s responsibility to destroy their VM. Upon deleting the VM within the ARC-P console, all VM data is deleted.

ARC-P Storage Device Decommissioning: When a hard drive fails within the ARC-P storage system, the device is securely erased using the NIST 800-88 Guidelines for Media Sanitation and placed within a locked media destruction bin. The media destruction bin is located within the dedicated, private cage

space that only cleared ARC-P personnel can access. All media within the media destruction bin is scheduled to be destroyed quarterly. Failed storage devices are never returned to the hardware manufacturer or vendor.

CSRA Data and Storage Device Decommissioning: CSRA disposes of all in-service and DR media per NIST 800-88. Media Sanitation requires media scheduled for destruction to be secured in a locked container in a secure location awaiting destruction. All media is destroyed per local site or data center standard operating procedure.

6.5.2 Compliance with Applicable Laws Related to Data Privacy and Security [8.5.2]

CSRA practices adherence to applicable laws of data privacy and security daily for our customers. We employ security software engineers to incorporate security and compliance with all applicable data privacy and security laws by auditing each contract and solution we deliver to our customers. Microsoft and Amazon commit to the same rigors as they deliver via CSRA on the NASPO ValuePoint Cloud Solutions MSA.

CSP FedRAMP and other national and international standards certifications establish our base compliance framework to applicable laws for data privacy and security. Cyber security governance models, policies and controls remain in place at each CSP and each customer inherits them per NIST guidance. As systems are integrated into ARC-P, Microsoft Azure, or AWS cloud infrastructures, compliance responsibilities are incorporated in project planning, execution, and delivery assurance. By coupling governance-focused, audit-friendly features with applicable state compliance or audit standards, compliance is built to the standards of our cloud integrations from planning through delivery. Our governance-based approach helps Participating Entities establish and operate compliant business applications in secure and auditable control environments.

6.5.3 Plan to Not Access Purchasing Entity's User Accounts [8.5.3]

CSPs and cloud customers share the security and compliance responsibilities as cloud computing customers build systems on top of cloud infrastructure. In an IaaS, Purchasing Entities control how they architect and secure their applications and data put on the infrastructure, while CSPs provide services on a secure platform and provide additional security features. The level of CSP and customer responsibilities in this shared responsibility model depends on the cloud deployment model (see the NIST Definition of Cloud Computing models).

CSP Responsibility: CSP operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities where the services operate.

Purchasing Entity Responsibility: Purchasing Entities assume responsibility and management of the guest operating system (including updates and security patches); other associated application software; configuration of the CSP provided security group firewalls; and other security, change management and logging features.

CSRA and its vendor do not access customer data. Purchasing Entities can choose how they store, manage and protect their data. CSRA promotes client understanding of the following fundamentals regarding data ownership and management in the cloud shared responsibility model. Purchasing Entities:

1. Own their data.
2. Choose the Cloud in which to store data—it does not move unless the Entity decides to move it.
3. Download or delete their data whenever they like.
4. Consider their data sensitivity requirements for data in transit at rest.

PaaS works similarly to IaaS but CSRA and its vendors manage the OS in PaaS. For SaaS, the vendors manage everything with the exception of accounts and some software configuration settings. CSRA does

not access the customer's account unless requested by the Purchasing Entity for account management task such as creation, password resets and deletion.

6.6 PRIVACY AND SECURITY [8.6]

An organization's security objectives are a key factor for decisions about outsourcing IT services and, in particular, decisions about transitioning organizational data and applications to a public cloud computing environment. CSRA recommends a risk-based approach in analyzing available security and privacy options, and deciding about placing organizational functions into a cloud environment. The IT governance practices of the organizations that pertain to the policies, procedures, and standards used for application development and service provisioning, and the design, implementation, testing, use, and monitoring of deployed or engaged services should extend to cloud computing environments.

CSRA offers governance, compliance and risk management capabilities through its Government Compliance and Risk Management Service (CSGS). Based on RSA's Archer tool, CSGS provides clients a single screen that gathers information from throughout the enterprise including relevant industry compliance status, incident response management and enterprise management. CSGS aligns with the government NOSC capabilities so its services can support SOC-managed government information systems.

This offering aligns with the ITC Government NOSC capabilities so its services remain available to support SOC-managed government information systems and government information systems managed by a government or a managed security service provider (MSSP) SOC. Through this offering, CSRA provides a low-cost unified approach in addressing government cyber security laws, regulations, and policies.

Ownership & Control of Customer Content

- Access: Purchasing Entities manage access to their content
- Security: Purchasing Entities choose how they secure their content. Providers offer encryption for customer content in transit or at rest with the option to manage encryption keys
- Assurance: Cloud providers have developed a security assurance program using global privacy and data protection best practices in order to helping Purchasing Entities establish, operate and leverage a standard security control environment

6.6.1 Compliance with NIST and Other Relevant Standards [8.6.1]

The Federal Information Security Management Act (FISMA) requires government agencies to improve the security of IT systems, applications, and databases. Each agency must develop, document, and implement a program to provide security for the data and IT systems that support its operations and assets. The NIST develops IT security standards and guidelines for FISMA. Federal agencies must follow these rules that require compliance reporting by each agency.

Federal government agencies follow an eight-step process for achieving FISMA compliance derived from NIST documentation. The security controls set forth by COBIT combined with the infrastructure processes of ITIL provides an effective framework for FISMA compliance as published by NIST.

The following lists FISMA certifications the CSPs attained. Each of our CSPs has obtained FISMA certification and compliance with NIST and other relevant security standards. Each cloud provider follows the FISMA accreditation and certification processes required to maintain their FISMA accredited state.

AWS: <http://aws.amazon.com/compliance/published-certifications/>

Microsoft Azure: <https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx>

ARC-P: In December 2012, the Joint Authorization Board (JAB) under FedRAMP granted the ARC-P Community IaaS cloud offering its first government-wide authority to operate (ATO) at the FISMA Moderate Impact Level. The FedRAMP JAB comprises the chief information officers from the DoD, Department of Homeland Security and the General Services Administration. According to its charter, the JAB grants provisional authorizations to CSPs based on evaluations of authorization packages, FedRAMP

accredited third-party assessment organization (3PAO) security assessment results, and FedRAMP PMO. In June 2013, the JAB added ARC-P Private IaaS to this authorization.

In April 2013, the Defense Information Systems Agency (DISA) issued ARC-P IaaS a DoD Provisional Authority to Operate. ARC-P IaaS has authorization at DoD Impact Levels 1 & 2 for Unclassified Public Information and Unclassified Private Information. DISA Field Security Operations assessed the ARC-P IaaS offering using the DISA-developed DoD cloud security model that it performed for an additional 23 controls and control enhancements from NIST SP 800-53 revision 3, beyond the FedRAMP Moderate baseline. DISA also reviewed of the standing ARC-P FedRAMP security authorization package.

In July 2015, Autonomic Resources committed to completing the FedRAMP high pilot with GSA and the FedRAMP JAB. ARC-P has increased the security posture of ARC-P IaaS offerings to meet the FedRAMP high baseline. Our 3PAO assessment was completed in November 2015, and the FedRAMP JAB has all documentation under review. A new provisional ATO acknowledging the move to FedRAMP high is anticipated in April 2016. In October 2015, the FedRAMP JAB granted Autonomic Resources a government wide ATO for ARCWRX PaaS at the FISMA Moderate Impact Level.

6.6.2 Security Certifications Held [8.6.2]

Our cloud providers track and complete attestations, and compliance certifications that confirm control placement to help enable cloud solutions for government organizations. Compliance represents a set of requirements for government agencies that address IT security and privacy considerations.

The following links to each team cloud provider list the security certifications and attestations each vendor earned.

AWS: Details on any certification, attestation or credentials are available from AWS. AWS certifications are published at: <http://aws.amazon.com/compliance/published-certifications/>

Microsoft Azure: Details on any certification, attestation or credentials are available from the Microsoft Compliance Trust Center: <https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx>

Autonomic Resources ARC-P: In December 2012, the FedRAMP JAB granted the ARC-P Community IaaS cloud offering its first government-wide authority to operate (ATO) at the FISMA Moderate Impact Level. In April 2013, DISA issued ARC-P IaaS a DoD Provisional Authority to Operate. ARC-P has obtained all FedRAMP certifications necessary to support Purchasing Entities.

6.6.3 Security Practices in Place [8.6.3]

CSRA meets physical and information system security requirements by providing a low-risk, flexible, FedRAMP and NIST-compliant architecture. We implement the architecture in a cloud environment using a layered security model that pays attention to the physical and logical separation of computing environments. Our security approach follows a layered security model (stack) as a means to visualize the complexity of cyber security challenges, **Exhibit 6-9** depicts our layered security model with a “security stack” that combines people, processes, and technology as integral parts of any service. We apply the layered security model to the cloud

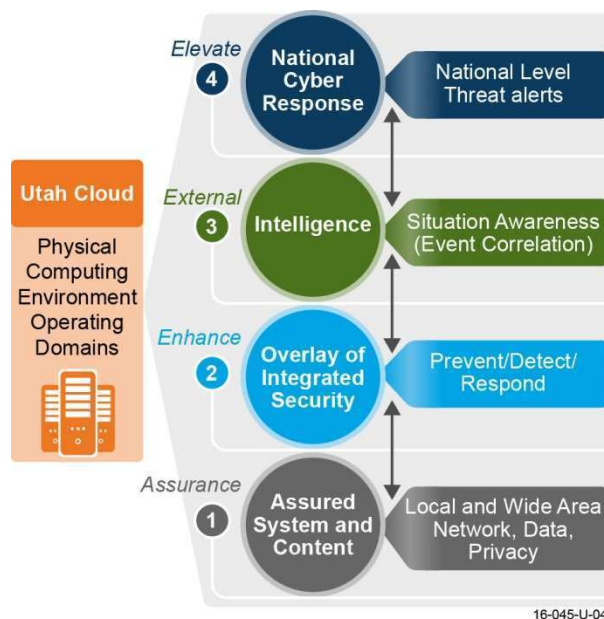


Exhibit 6-9. CSRA's Layered Security Model. We apply the layered security model to the cloud operating domains for security solution completeness

operating domains assuring the completeness of the security solution. The cyber security blueprint that creates the cloud operating domains proves integral to an ecosystem where the complete set of architectures is made secure and sustainable by design.

The security stack does not define inviolable boundaries or gates, nor does it imply that one layer of security cannot exist without another. Only by addressing all four layers can we balance the benefit and risk of cyber systems, and better understand how to achieve the right balance of prevention and impact. We address Purchasing Entities' security requirements in terms of the layered solution required to protect against evolving cyber security threats for tenant applications, physical computing environments, and the data center facilities providing cloud computing services.

In **Section 6.6.10**, we examine how our security model applies to the technical architecture that facilitates Purchasing Entities creating cloud services with confidence. We provide a cost-effective cloud brokering business model implemented in a secure hybrid cloud services approach that our Agility Platform monitors and manages.

6.6.4 Data Confidentiality Standards and Practices in Place [8.6.4]

Data confidentiality standards and practices address protections of data and systems including access management, administrative controls, including rules of behavior, awareness training, and incident response. The policies and processes of our cloud providers and data centers reflect data confidentiality to protect information from improper disclosure while protecting the secrecy and privacy of sensitive data. We will protect the sensitivity of Purchasing Entities' data so intellectual property and reputation remains safe, and data related to individuals is not released in violation of privacy policy regulations. Our standards and practices reflect our cloud vendors' compliance and their environments that conform to NIST standards for security and privacy. FISMA emphasizes NIST standards for security and privacy in its controls for low, medium, and high security environments certified for each cloud provider. From a cloud vendor's perspective, the provider does not access customer data, and Purchasing Entities can choose how they store, manage and protect their data.

Access Management: Per NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, access that administrators have to stored data is managed and reviewed. Access controls include separation of duties, least privilege, monthly access reviews, and auditable events. All access to sensitive information is requested, approved, and reviewed based on job function requirements and need-to-know. In addition, all access to sensitive information is logged and monitored.

Administrative Controls: Operational and administrative safeguards include security policy and procedures, training, and education for our internal employees. Sanctions are applied and commensurate with the level of violation and aligned with federal, state, and local law.

- **Rules of Behavior:** All employees annually sign Rules of Behavior, which address privacy and data confidentiality internally and for our customers, and includes social media responsibilities. Employees must use approved laptops to access their information and systems within the ARC-P Security Boundary. Assigned equipment remains secure at all times and protected using antivirus and firewall software. Personally owned equipment is not allowed.
- **Privacy and Security Training:** Awareness efforts aim to change behavior or reinforce confidentiality practices. The efforts include methods informing staff of new scams, and providing updates on topics such as government data breaches and their effect on the organization.
- **Incident Response:** Incident response policies, procedures, and plans cover data-breach procedures and data spillage per DoD 5240.

Technical Controls: Our Identity and Access Management solution leverages ServiceNow and Agility Platform Identity Access Management capabilities. The process starts with the ServiceNow administration team configuring the ServiceNow catalog to pass user authentication information for users to the Agility Platform. On the Agility Platform, we create user authorization tables for each CSP hosting

application Purchasing Entities use. The act of individual Purchasing Entities specifying catalog selection privileges with Authorized User Access Request forms ties ServiceNow catalog selections through Agility to the CSP cloud instances. The Agility system administrators update the system user store in accordance with the Security Credential Management Plan, which establishes guidelines for Purchasing Entities' user access.

6.6.5 Third-Party Attestations, Reports and Security Credentials [8.6.5]

The following links to each team cloud provider list the security certifications and attestations each vendor earned.

AWS: Details on any certification, attestation or credentials are available from AWS. AWS certifications are published at: <https://aws.amazon.com/compliance/published-certifications/>

Microsoft Azure: Details on any certification, attestation or credentials are available from the Microsoft Compliance Trust Center: <https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx>

Autonomic Resources ARC-P: In December 2012, the FedRAMP JAB granted the ARC-P Community IaaS cloud offering its first government-wide authority to operate (ATO) at the FISMA Moderate Impact Level. In April 2013, DISA issued ARC-P IaaS a DoD Provisional Authority to Operate. ARC-P has obtained all FedRAMP certifications necessary to support Purchasing Entities.

CSRA: CSRA stores no client data for Purchasing Entities.

6.6.6 Logging Processes [8.6.7]

Cloud providers offer logging processes as services or capabilities; the content and fields that are logged are particular to the log service purchased. The logging and monitoring of API calls are key components in security and operational best practices, and requirements for industry and regulatory compliance. Purchasing Entities can leverage features, capabilities, and third-party tools to monitor their instances and manage or analyze log files.

Our SOC collects log files created during the creation of a cloud instance (beginning with ServiceNow through instance creation on the cloud providers) and positions them in Layer 3 of our security framework. Layer 3 acts and as a command and control center to provide a common operating picture of CSRA data center operations. It involves collecting state data, control-based evidences, and dynamic data logging at the enterprise level. Intelligence gathered from the layers below correlate at the enterprise level to provide context into the threat landscape. Correlations of threat indices are then normalized and a view can be provided to upper layer for use in threat analysis.

The log collection service proves pivotal to the data feeds CSRA SOC provides. The SOC SIEM collects lower-level security layer data from different sources. SOC analysts use information from the collected data feeds from the lower layers (1 and 2) to present on a dashboard at Layer 3 to decision makers. The Layer 3 data picture presents a unified holistic view of an organization's Risk, Compliance and Security posture in order to make the decisions to protect an organization and pass information to Layer 4 of the Security Stack. See Section 6.6.3 for our layered security model.

6.6.7 Restricting Visibility of Cloud Hosted Data and Documents [8.6.7]

Identity and Access Management (IDAM), a Web service cloud providers offer, enables Purchasing Entities to manage users and user permissions in their cloud instances. The IDAM service targets organizations with multiple users or systems that use cloud provider products. With cloud provider IDAM services, Purchasing Entities can centrally manage users, security credentials such as access keys, and permissions that control which resources users can access.

Permissions let Purchasing Entities specify who has access to cloud instance resources and which actions they can perform on those resources. Every IDAM user starts with no permissions. Users are granted individual permissions on a case-by-case basis; alternatively, users can be added to a security group that has the desired permissions.

For the Microsoft Azure cloud environments, Purchasing Entities have the ability to extend their Active Directory and any other on-premises directories to Azure Active Directory to enable single sign-on for all cloud-based applications. User attributes can be automatically synchronized to cloud directories from on-premises directories. Azure Active Directory also offers developers an effective way to integrate identity management into applications. Industry-standard protocols such as SAML 2.0, WS-Federation, and OpenID Connect make sign-on possible on platforms such as .net, Java, Node.js, and PHP. The REST-based Graph API enables developers to read and write to the directory from any platform. Through support for OAuth 2.0, developers can build mobile and Web applications that integrate with Microsoft and third-party Web APIs, and build their own secure Web APIs. Open-source client libraries are available for .net, Windows Store, iOS, and Android, with additional libraries under development.

For client-managed applications and environments (IaaS, SaaS, PaaS), Purchasing Entities assume responsibility for the IDAM accessibility of their cloud managed applications and data.

6.6.8 Security Incident Notification Procedures [8.6.8]

Each cloud provider has implemented methods of external communication to support its customer base and the community. The mechanisms in place allow the customer support team to receive notifications of operational issues that impact the customer experience. Our cloud vendors provide a service health dashboard maintained by the cloud providers' customer support teams to alert customers to any broad-impact issues. The service health dashboard provides Purchasing Entities with security and compliance details about their cloud instance. Purchasing Entities can also subscribe to support offerings that include direct communication with the customer support team and alerts to any customer-impacting issues.

CSRA SOC analysts provide Purchasing Entities with formal incident reports and classification for the intrusion investigation and incident, ensuring appropriate handling of need-to-know and sensitivity. CSRA SOC analysts work with Purchasing Entities' SOC and NOSC personnel and with cloud vendor response personnel. The incident response site lead provides periodic updates to senior CSRA leadership. Senior CSRA management communicates with Purchasing Entities affected by the breach.

Incidents are reported via the incident report form. The Site Lead ensures incident reports identify Who, What, When, Where, Why, and How. Incident summaries are included in the CSRA SOC daily report or other approved rollup reporting. Incident reports are always entered into the ServiceNow ticketing system, the official historical record for troubles of any kind. Any user can contact the help desk to ensure an incident or problem has been reported.

6.6.9 Physical and Virtual Zone of Control Security Architectures Security Controls [8.6.9]

Each cloud provider provisions a logically isolated section of the cloud for IaaS, SaaS, and PaaS environments in a client-defined virtual network (VNet). VNet represents a customer network in the cloud. It is a logical isolation of the cloud dedicated to a Purchasing Entity's instance. Each Purchasing Entity can control the IP address blocks, DNS settings, security policies, and route tables within this network. A Purchasing Entity can also further segment its VNet into subnets, and launch VMs and cloud services (PaaS role instances). Additionally, Purchasing Entities can connect the VNet to their on-premises network using one of the connectivity options available from the cloud providers. Each Purchasing Entity can expand its enterprise network into the cloud with complete control on IP address blocks.

For example, a Purchasing Entity can create a public-facing subnet for Web servers with access to the Internet, and place backend systems such as databases or application servers in a private-facing subnet with no Internet access. Purchasing Entities can leverage layers of security, including security groups and network access control lists, to help control access to instances in each subnet.

6.6.10 Security Technical Reference Architectures [8.6.10]

CSRA will help the Participating and Purchasing Entities navigate cloud services with confidence. We provide a cost-effective cloud brokering business model implemented in a secure hybrid cloud services approach that our Agility Platform monitors and manages.

Our solution simplifies the challenge of securing, monitoring and managing services across CSPs by using a single common user interface that provides real-time control, performance, and situational awareness across all client cloud environments. The Agility Platform provides the interface.

CSRA's ServiceMesh Agility Platform, shown in **Exhibit 6-10**, has automation and orchestration as the defining features established in the NIST Cloud Standards Roadmap (NIST SP 500-291) for a Cloud Broker; which states, "The ability to provide a single consistent interface to multiple differing providers, whether the interface is for business or technical purposes." We use the Agility Platform to manage hybrid cloud cross-platform portability while implementing NIST and state cloud policies. We will use Agility Platform to provide unified management, operations, and security policy control over our enterprise-scale hybrid cloud solution. This drives application portability and consistent security controls across FedRAMP-certified CSPs. General Electric, Visa, UBS, American Express, Swisscom, BestBuy, and Commonwealth Bank use Agility Platform.

Using our security practices model as described in **Section 6.6.3**, we apply our layered vision to the capabilities of the Agility Platform to provide a consistent architecture applicable to creating IaaS, SaaS, and PaaS solutions on the selected cloud providers.

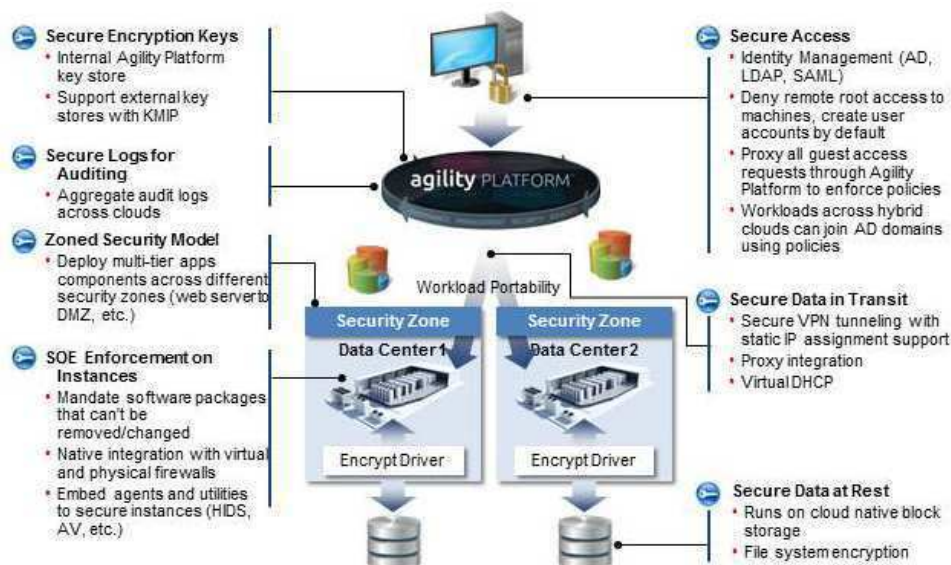


Exhibit 6-10. ServiceMesh Agility Platform. Agility Platform provides a multilayered approach that allows state organizations to create their preferred security system.

Layer 1

Layer 1, Assured System and Content, addresses information-communications technologies (ICT) architected and designed to operate securely within the NIST/FIPS compliant ServiceMesh environment. Accordingly, the required degree of security is applied to the appropriate IaaS, SaaS and PaaS computing environment.

Cloud Based Security Groups and Identity Access Management

Agility Platform policies govern which applications and instance types can be placed in the different cloud environments, including which users and groups are authorized to create an instance. These policies dictate which workloads can be deployed to authorized cloud environments. For example, sensitive

applications may be required to run in a private cloud, a hosted private cloud, or other specified environment.

The Agility Platform provides role-based access control with over 200 fine-grained rights corresponding to user actions within the platform. User credentials from directories including Microsoft Active Directory, and single sign-on services like SAML2.0 or API interfaces can be conveniently mapped to these custom-defined project roles.

Our Identity and Access Management solution leverages ServiceNow and Agility Platform Identity Access Management capabilities. The process starts with the ServiceNow administration team configuring the ServiceNow catalog to pass user authentication information for users to the Agility Platform. On the Agility Platform, we create user authorization tables for each CSP hosting application Purchasing Entities use. The act of individual Purchasing Entities specifying catalog selection privileges with Authorized User Access Request forms ties ServiceNow catalog selections through Agility to the CSP cloud instances. The Agility system administrators update the system user store in accordance with the Security Credential Management Plan, which establishes guidelines for Purchasing Entities' user access.

Data Integrity and Confidentiality

Agility Platform policies govern which application workload and instance types may be placed in different cloud environments, including which users and groups are authorized to create an instance. Access management included in the first layer of Agility Platform's multilayered governance and security model enforces data confidentiality. This includes the ability to create custom policies based on an extensible meta-model that enables consumption resources based on custom parameters.

We achieve data integrity by forcing access control policies so users can only change information and programs in an authorized, role-appropriate manner appropriate. These policies can also dictate that certain workloads can only be deployed to authorized cloud environments. For example, sensitive applications may be required to run in a private cloud or other specified environment. This establishes controls that support end users making appropriate choices when placing workloads and instances in a cloud choice by enforcing access control and/or provisioning constraint policies.

All nonpublic operating domains are operated in virtual private clouds that extend their associated client environment to client users. All CSRA CSPs support the creation of virtual private clouds (VPCs) that allow access to resources in those VPCs only from a Purchasing Entities' network connected to the VPC – not from the Internet.

Layer 2

Layer 2, Overlay of Integrated Security, the traditional "security" layer, comprises planes across the network and application layers. Forms in the layer range from engineered-for-purpose hardware to software evaluation tools. We add defense-in-depth here based upon client sensitivity to risk.

Separation: Physical, Logical Operating Domain, Network and Virtual Machine

As described in **Section 6.6.9**, our cloud providers physically separate network traffic at every level. Operating domains are segregated by VLANs and at the environment level within operating domains governed by the Agility Platform. Security at the network level occurs in virtual and physical realms. We use Agility Platform policies to govern which application workload and instance types may be placed in the different cloud domain environments, including which users and groups have authorization to create an instance.

Layer 3

Layer 3, Intelligence, a "decision support system," layer, provides a common operating picture and communication mechanisms that allow easy data-source access, and conceptualize outcomes based on data analysis.

Intrusion Detection and Prevention

Our SOC Operations Control Center (OCC) provides threat coverage for servers, network devices, firewalls and internal networks. This service combines signatures, protocol validation, anomaly detection, and behavioral analysis to provide network IPS protection. By filtering 90% of incoming traffic without requiring deep inspection, the IPS engine inspects for attacks only on relevant sections of the traffic to reduce overhead and increase accuracy.

A combination of vendor products that provide an integrated network security solution powers our OCC, which allows us to deliver network security including the ability to: report on network policy compliance; defend against the latest attacks; perform deep level packet inspection; monitor attacks and performance issues; provide real-time alerts; and enforce security policies. We understand maintaining situational awareness of Purchasing Entities' networks, and we ensure the monitoring interface will provide separate reporting with common visibility to enhance the response to any cyber incident.

The OCC monitors network traffic performance and provides alerting and reporting on network metrics. The OCC also provides the following services: security monitoring and analysis of network traffic with IDS/IPS appliances; sensor event collection incident investigations in real-time employing advanced query and analysis tools; incident reporting to Purchasing Entities; and notification and escalation of critical alerts.

Layer 4

Layer 4, National Cyber Response, leaves the topic of network security. Threats operate in Internet time. The needed exchanges of threat information cannot wait for bureaucratic time. CSRA ties Layer 4 into Purchasing Entities' risk management by integrating independent validation and verification and other threat information through the RSA Archer platform to provide a more accurate risk perspective.

6.6.11 Security Procedures for Employees Who Have Access to Sensitive Data [8.6.11]

As discussed in **Sections 6.3.2** and **6.3.3**, CSPs provide secure infrastructure components, services and features to enhance security. CSPs meet national and international standards certifications with compliance that addresses applicable laws for data privacy and security. Controls in place at each CSP limit employee access to customer data. These governance elements help Purchasing Entities establish and operate compliant business applications in a FedRAMP-approved security environment. In summary, each CSP implements technical and physical controls to prevent unauthorized access to or disclosure of customer content. To provide continued compliance, independent assessors conduct impartial assessments of organizational information systems.

Additionally, CSPs give Purchasing Entities ownership and control over their content through tools that allow them to determine where to store their content, how to secure their data in transit or at rest, and the services and tools that protect access for their users. CSPs provide a set of access, encryption, and logging features to help customers protect their data. CSPs do not have access or use Purchasing Entity content for any purpose other than as legally required.

CSPs publish a Privacy Policy that describes how each CSP collects and uses information that Purchasing Entities provide in the connection with the creation or administration of accounts. This privacy policy applies to Purchasing Entities' account information and does not apply to the content that Purchasing Entities store on CSP systems. CSPs do not disclose, move, access or use customer content except as provided in the agreement with each Purchasing Entity. CSPs will not disclose customer content unless required to do so to comply with the law or a valid and binding order of a governmental or regulatory body.

CSPs have organized monitoring processes and capabilities to detect and prevent the unauthorized disclosure of sensitive information. CSPs have created internal threat programs that limit employee access to information; address centralized information integration, analysis, and response; employee insider

threat awareness training; and the monitoring of user activity on customer computing instances. These policies and training efforts are employed for safeguarding Purchasing Entities' information.

6.6.12 Security Measures and Standards for Data at Rest and In Transit [8.6.12]

Federal organizations are responsible for the information security risk incurred by the use of information system services that external cloud providers offer. To meet this requirement, CSPs must obtain and maintain FedRAMP certification. CSPs provide a risk management foundation to achieve that compliance through their FedRAMP accreditation. CSPs take a two-pronged approach to support the currency of compliance controls, measures and standards and that each maintains a compliance framework. CSP service offerings reflect the security measures for securing data at rest and in transit. CSP share security measures with their customers, who retain ultimate responsibility for data security.

Certifications and attestations, and third-party audits independently validate CSP vendors to demonstrate that these controls deliver compliance. In-scope services within the cloud offerings meet key international and industry compliance standards, such as ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1 and SOC 2. The Participating Entity determines whether services comply with the laws and regulations applicable to their business and legal requirements. To make these assessments, each CSP supplies service and product specifics and its security and compliance programs, including audit reports and compliance packages. Purchasing Entities can verify implementation of the controls by requesting audit results from the certifying third parties, through each CSP account representative, or through the CSRA Contract Manager.

6.6.13 Policies and Procedures for Notification of a Data Breach [8.6.13]

Our NOSC in Bossier City, La., offers Purchasing Entities a range of security services to include 24x7 security monitoring, anti-virus services, intrusion detection services, threat analysis, threat mitigation, and event remediation services. To provide cost efficiency without compromising security, CSRA's NOSC services remain available in a leveraged "SOC as a Service" managed services model.

We will educate Participating and Purchasing Entities on our security services available through NASPO ValuePoint Cloud Solutions, and discuss what options and configurations would prove most appropriate for project and security needs. Throughout the acquisition cycle, we will recommend, discuss, and validate policies, procedures, and SLAs as they apply to laws, regulations, and organizational policies unique to each project, and establish a Purchasing Entity cyber security point of contact (POC). Our NOSC Manager Wayne Maddock and Director of Cybersecurity Samuel Toler have established CSRA cyber security policies and procedures that include breach notification and mitigation based on the guidelines set forth in NIST Special Publication 800-53, the procedures defined in the US Computer Emergency Response Team (US-CERT) Incident Response Playbook, and the policies described in the FISMA.

When CSRA identifies a potential breach of a network hosted by a Purchasing Entity, CSRA notifies the Purchasing Entity's cyber security POC and provides supporting mitigation procedures as specified in the project contract. When CSRA hosts Purchasing Entity networks or data, CSRA will assign a lead IA analyst at project kickoff who tailors our SOPs and guidelines to provide direction for notification and mitigation actions including: escalation chain; pre-approved mitigation actions; end-user and cardholder communications plans; and approval authorities in the event of a potential data breach. We implement all notification and mitigation procedures and policies in accordance with FISMA, NIST, and US-CERT guidelines.

6.7 MIGRATION AND REDEPLOYMENT PLAN [8.7]

CSRA offers the benefits from our vast cloud migration experience to our customers. We created this approach from existing process and products and tailor it specific to the Purchasing Entity needs.

CSRA has modernization and migration process reflecting industry best practices and our expertise. Our core processes, artifacts, and decision criteria drive all migration planning and execution activities across Physical-to-Physical (P2P), Physical to Virtual (P2V) and Virtual to Cloud (V2C) migrations. We have used these processes in successful migrations, including the CMS Development Environment Consolidation Contract (DECC). As part of the DECC effort, CSRA migrated over 200 legacy systems to a new target environment on schedule and under budget.

CSRA also uses industry-best practices including ITIL v3 processes for migration—change, configuration, release management to lower risk, define customer process integration points and activities, and ensure predictable and sustainable results.

6.7.1 Maintaining End of Life Activities [8.7.1]

Our lifecycle procedures vary based on the service-level definition of each service.

Our hybrid cloud model security policies for data retention adhere to industry-best practices and federal government requirements. Solutions range from physical (i.e., demagnetization and destruction of storage media) to logical (cryptographic overwriting of disk space). CSRA cloud and traditional infrastructure disk and data destruction requirements are at the customer's behest. CSRA works on a program-by-program basis to identify a solution and adhere to required policy. For example, when contractors leave control of a DoD program, DoD requires them to use DoD-mandated tools to sanitize its hard drives to ensure residual data remains inaccessible for compromise. Regarding permanent removal of data from shared storage media, CSRA's system architecture supports DoD-standard wipe utilities for disks in operation, and we follow DoD sanitization procedures for standalone drives removed from the environment.

Risk and Mitigation Strategies for DR – CSRA experience brings risk mitigation strategies for the top five risks in collocation and cloud computing services delivery. Our corporate cloud service delivery model supports the automatic failover and restart of tenant applications to back up processing functions within the same cloud or across multiple clouds. Purchasing Entities may need cloud computing services and facilities capable of withstanding localized failure without disruptions, facilitating automated failover and restart of tenant applications, and replicating data using a sound technical approach. Cloud operations and monitoring itself must provide continuity of operations of cloud online and monitoring services. CSRA's hybrid cloud and co-location solution incorporates redundancy in technology stack components and potential providers, and seamless migration of services through the brokering interface. Our CSP partners have exemplary records in combating infrastructure failures. CSRA's solution has redundancy and resiliency at every level to eliminate the impacts of planned and unplanned service interruption.

Portability – A cloud broker model, such as CSRA's ServiceMesh Agility Platform, enables the data portability of workloads and platform metadata. The Agility Platform provides this next layer of flexibility for tenant applications by enabling blueprints—plans defining and governing technical and operating aspects of application workload that include scalability rules and permissions. When these blueprints are implemented, the operational hypervisor permits resizing resources allocated to an existing instance, such as increasing CPU or memory allocation, while Agility enforces policies to automatically optimize resource consumption based on usage.

CSRA's Migration Expertise

- For DHS, CSRA migrated 17 data centers into a single 63,000 sq.ft. facility including one of the first government-owned, contractor-run FISMA moderate private clouds
- For the CMS Development Environment Consolidation Contract, CSRA used FuturEdge to move over 200 legacy systems to a new target environment on schedule and under budget
- For the FAA, CSRA migrated 80,000 FAA and DOT employees and contractors to the Office365 Cloud (Outlook, Lync, and Proof Point) solution

The Agility Platform abstracts the underlying CSP hypervisor architectures so applications and workloads can be deployed among different clouds with no recoding or refactoring. With the Agility Platform which is offered as an optional service, Purchasing Entities can design and deploy cloud portable, multitier applications and platforms; monitor and manage hybrid workloads; and extend, enhance, and automate the application development and operations (DevOps) environment.

6.7.2 Orderly Return of Back Data [8.7.2]

Purchasing Entities own and control their own data. The Purchasing Entity may at any point download or delete their data on any CSRA solution. Before decommissioning a system or account, the Purchasing Entity should ensure the any data that they require transfers to another system, cloud provider or their own data center. With regard to Office 365 Services, Microsoft Azure Core Services, Microsoft Dynamics CRM Online Services, and Microsoft Intune Online Services, Microsoft provides customer administrators access to their customer data in the online services at all times during the term the subscription, and for at least 90 days thereafter (but for no more than 180 days). Where the modality of the online service is applicable and as described in the applicable service documentation and service descriptions at the time, Purchasing Entities can download customer data in the online services in a common industry or published Microsoft format during the term of each subscription, and for a 90-day “limited functionality” period following expiration (as set forth in the Online Services Terms). For large amounts of data that needs to transfer where moving the data over a network would prove long and expensive, some of our solutions have the option to put the data on to a hard drive and mail it to the Purchasing Entity. For this option, the data is encrypted before it’s placed on the hard drive to ensure the security of the data in transit. The encryption keys are provided separately to the Purchasing Entity.

6.8 SERVICE OR DATA RECOVERY [8.8]

Cloud computing takes a different approach to data recovery. With cloud virtualization such as CSP ARC-P, data is encapsulated into a single-software bundle or virtual server. AWS and Microsoft Azure separate the server image from Purchasing Entity data. In this case, the operating environment is created from a containerized image and the data connected to the operating environment. With a cloud provider, recovery becomes more cost-effective with faster times.

6.8.1 Method of Response [8.8.1]

Our response to outages and failures will vary with the cause and nature of the incident, but in all cases CSRA will inform affected Purchasing Entities as soon as we know of a service outage. Throughout the process, we will keep Purchasing Entities up to date with status, possible options, and expected recovery time. In the event of extended down time or in cases of extensive data loss, the sections below discuss data storage and recovery.

6.8.1.1 Extended Downtime [8.8.1 (a)]

In the case of extended down time, we enter the decision cycle to execute DR and continuity planning or continue to wait for service or application restoration. In these cases, the choice of storage and data backup becomes important to the decision making cycle. Below, we discuss data recovery for each of the cloud providers.

AWS uses distinct and geographically diverse Availability Zones (AZs) engineered to remain isolated from failures in other zones. This AWS feature enables Purchasing Entities to protect applications from the failure of a single location, resulting in cost savings and increased agility to change and optimize resources during extended down time.

AWS offers the following capabilities:

- Fast, disk-based storage and retrieval of files
- No tape media or associated tape backup software

AWS Storage: Purchasing Entities choose a storage mechanism depending on the criticality of their mission. Services and features that support data migration and durable storage enable Purchasing Entities to restore critical data to AWS when required.

Amazon Simple Storage Service (Amazon S3) provides a storage infrastructure designed for mission critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities within a region, designed to provide durability.

Amazon Glacier provides low-cost storage for data archiving and backup. Objects (Amazon Glacier refers to them as “archives”) are optimized for infrequent access, for which retrieval times of several hours are adequate. Amazon Glacier is designed for the same durability as Amazon S3.

Amazon Elastic Block Store (Amazon EBS) provides the ability to create point-in-time snapshots of data volumes. Purchasing Entities can use the snapshots as the starting point for new Amazon EBS volumes, and can protect data for long-term durability because snapshots are stored within Amazon S3. After a volume is created, Purchasing Entities can attach the volume to a running Amazon Elastic Compute Cloud (Amazon EC2) instance. Amazon EBS volumes provide off-instance storage that persists independently from the life of an instance and is replicated across servers in an AZ to prevent the loss of data from the failure of any single component.

AWS Import/Export accelerates moving large amounts of data into and out of AWS by using portable storage devices for transport. AWS Import/Export bypasses the Internet and transfers data onto and off of storage devices by means of the high-speed internal network of Amazon. For data sets of significant size, AWS Import/Export is often faster than Internet transfer and more cost-effective than upgrading connectivity. Purchasing Entities can use AWS Import/Export to migrate data into and out of Amazon S3 buckets and Amazon Glacier vaults or into Amazon EBS snapshots.

AWS Storage Gateway connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between on-premises IT environment and the AWS storage infrastructure.

AWS Backup and Restore: Amazon S3 is an ideal destination for backup data that might be needed to perform a restore. Transferring data to and from Amazon S3 is typically done through the network, and is therefore accessible from any location. Many commercial and open-source backup solutions integrate with Amazon S3. Purchasing Entities can use AWS Import/Export to transfer large data sets by shipping storage devices to AWS. For longer-term data storage where retrieval times of several hours are adequate, there is Amazon Glacier, which has the same durability model as Amazon S3. Amazon Glacier and Amazon S3 can be used in conjunction to produce a tiered backup solution.

Microsoft Azure: Microsoft Azure Government backup’s client Azure IaaS VMs use Azure Backup. Microsoft Azure Backup Server, a feature of Azure Backup, protects workloads to disk and cloud for all Azure Government customers. Purchasing Entities can leverage this Microsoft Azure Backup Server to back up their key Microsoft workloads like SQL, SharePoint and Exchange to Azure. Microsoft Azure Backup server enables backup of Microsoft SQL Server, Hyper-V VMs, SharePoint Server, Microsoft Exchange and Windows Clients. Purchasing Entities with Tier 1 workloads like Microsoft SQL Server can benefit from Microsoft Azure Backup Server by choosing disk backups for better RPOs and RTOs. They can continue to backup to Azure for long-term retention using disk-cloud backup strategy.

Microsoft Storage: Azure Premium Storage delivers high-performance, low-latency disk support for I/O-intensive workloads running in Azure VMs. Attach one or more Premium Storage disks to a VM. Each VM can have 64 TB of storage, achieve 80,000 IOPS (I/O operations per second), and attain 2,000 MB-per-second disk throughput with low latencies for read operations. Premium Storage is available only for storing data on disks used by VMs.

Microsoft Backup and Restore: Azure Backup, a hybrid service, comprises components that work together to enable end-to-end backup and restore workflows to and from a backup data vault. The backup

data is stored in geo-replicated storage that maintains six copies of client data across two Azure data centers with 99.9% service availability. Once initial seeding completes, only incremental changes are sent at a defined frequency. Built-in features, such as compression, encryption, longer retention, and bandwidth throttling, help boost IT efficiency. No capital expenditure is needed for on-premises storage devices. Azure Backup automatically allocates and manages backup storage using a pay-as-you-use consumption model. Azure Backup uses autoscaling capabilities with storage options. A locally redundant storage block blob is ideal for price-conscious clients, and geo-replication storage provides three additional copies in a paired data center.

ARC-P: ARC-P operates across two CONUS sites in an ACTIVE/HOT STAND-BY configuration; Ashburn, Va. and Atlanta, Ga. With the ACTIVE/HOT STAND-BY system in two separate data centers, the entire stack replicates every 15 minutes. If the system loses an entire data center, ARC-P can maintain normal operations without having to pull from a stored backup. ARC-P runs at a 99.9% uptime.

ARC-P Storage: VMs hosted in ARC-P can be configured with virtual disk snapshot schedules.

ARC-P Backup and Restore: Virtual disk snapshots are automatically copied from cluster primary storage to zone secondary storage and replicated to the DR peer of the region. Individual files can be restored from snapshot by performing a 'Create virtual disk from snapshot' operation and attaching the virtual disk to a VM. Files can then be copied out of the virtual disk.

Full ARC-P IT Continuity Planning (ITCP) may be activated if one or more of the following criteria are met:

1. The type of outage indicates ARC-P will stay down for more than one hour.
2. The facility housing ARC-P is damaged and may not be available within one hour.
3. Complete power failure of the Atlanta data center along with all redundant power systems. The Ashburn Internet circuit would automatically pick up as primary route for all traffic. The ARC-P ITCP team would failover to the hot standby site in Ashburn. Expected service outage would be ~60 minutes from ITCP activation.
4. Complete loss of the Atlanta data center due to natural disaster, homeland attack, or facility emergency. The Ashburn Internet circuit would automatically pick up as primary route. The ARC-P ITCP team would failover to the hot standby site in Ashburn. Expected service outage would be ~60 minutes from ITCP activation.
5. Imminent threat to the Atlanta data center would result in ITCP activation and preemptive failover to the hot standby site in Ashburn.
6. All other failures or outages at the Atlanta data center would result in automatic failover to redundant systems. All failures or outages at the Ashburn data center would not result in an outage of the customer environment. Expected customer VM service disruption would be a minimum of 15 minutes and a maximum of 60 minutes for any automatic failovers.

6.8.1.2 Unrecoverable Loss of Data [8.8.1 (b)]

We understand unrecoverable data loss as an error condition in the operating environment in when failures or neglect in storage, transmission, or processing destroys information. In the event of this corruption in a Purchasing Entity's cloud operating environment, an Entity would have to implement backup and DR equipment and processes to prevent data loss. In such a case, the Purchasing Entity would have to engage with the cloud instance vendor and open a priority ServiceNow help desk ticket to engage the appropriate CSRA personnel.

6.8.1.3 System Failure [8.8.1 (c)]

In the event of a system failure, we recommend executing the DR option for the affected CSP. Changing CSP region or availability data center provides the most effective response to a failure. Upon completion

of the DR process, efforts can begin to recover the primary site computing environment. Data recovery options are described in more detail in [Section 6.8.1.1](#). Each cloud provider has a different recovery process. We described them below.

AWS: Amazon EC2 service provides scalable computing capacity in the AWS GovCloud. Purchasing Entities use Amazon EC2 to launch virtual servers, configure security and networking, and manage storage. Amazon EC2 facilitates DR. Amazon EC2 provides Purchasing Entities the ability to place resources, such as instances and data in multiple locations (separate availability zones in the GovCloud regional data center). By launching instances in separate AZs, Purchasing Entities can protect applications from the failure of a single location. Each AZ is as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower-risk flood plains (flood zone categorization varies by Region).

Many public sector organizations realize the benefits of using AWS for continuity of operations (COOP)/DR of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports popular DR architectures from “pilot light” environments ready to scale up at a moment’s notice to “hot standby” environments that enable rapid failover.

Azure: A cloud deployment might cease to function due to a systemic outage of the dependent services or the underlying infrastructure. Under such conditions, a business continuity plan triggers the DR process. This requires the transfer of application users, data, and services to the new data center. It also involves the use of backup media or ongoing replication.

DR/COOP design applies the “availability set” pattern. For Azure deployments either via IaaS or PaaS, the servers should be assigned to an availability set. In a typical three-tier application (front end, application, and database), each tier represents a different availability set. This tells Azure that any VM instance in a given availability set can satisfy the same role as the other members of the set. As long as at least one of the members of that set takes requests then the application as a whole is also available. The availability set translates into Azure fault domains.

Azure provides two fault domains as unique sets of hardware in the Azure data center that share no single point of failure. Azure will automatically provision the VMs in an availability set to spread across these fault domains. Azure promises the customer that any physical failure inside of an Azure data center will at most impact half of the VMs for that set. In order to get the Azure 99.95% availability SLA from Microsoft Purchasing Entities must deploy their application in this pattern. The SLA is on the availability set and not the individual VM.

Azure’s Update Domains capability aligns with Microsoft’s goal of providing a secure and stable environment to host applications because the software inside Azure needs periodic updates. Patches may require virtualization hosts to reboot and there must be a design mechanism to ensure that the VMs hosting application have proper timing for the reboot activity. Azure provides five update domains by default and they can extend to 20. When deploying VMs into an availability set, Azure slots them into Update Domains as well.

Autonomics ARC-P: Autonomics ARC-P operates across two sites within the US in an ACTIVE/HOT STAND-BY configuration; Ashburn and Atlanta. With the ACTIVE/HOT STAND-BY system in two data centers, the entire stack replicates every 15 minutes. If the system loses an entire data center, ARC-P can maintain normal operations without having to pull from a stored back up.

VMs hosted in ARC-P can be configured with virtual disk snapshot schedules. Virtual disk snapshots are automatically copied from cluster primary storage to zone secondary storage and replicated to the disaster recovery peer of the region. Individual files can be restored from snapshot by performing a ‘Create virtual disk from snapshot’ operation and attaching the virtual disk to a VM. Files can then be copied out of the virtual disk.

6.8.1.4 Recovery and Restoration of Data within Four Business Hours [8.8.1 (d)]

Our cloud vendors recovery and restore computing environments recovery and restoration details for each vendor are:

AWS: Many public sector organizations use AWS for COOP/DR of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports four popular DR architectures from “pilot light” environments ready to scale up at a moment’s notice to “hot standby” environments that enable rapid failover.

Purchasing Entities can eliminate the need for additional physical infrastructure, off-site data replication, and upkeep of spare capacity. AWS uses distinct and geographically diverse Availability Zones (AZs) engineered to remain isolated from failures in other AZs. This AWS feature enables Purchasing Entities to protect applications from the failure of a single location, resulting in cost savings and increased agility to change and optimize resources during a DR scenario.

One of the following AWS services can help meet recovery time objective (RTO) of within four hours or faster:

- **Warm Standby Solution:** The term “warm standby” describes a DR scenario in which a scaled-down version of a functional environment always runs in the cloud. It further decreases recovery time because, in this case, some services always run. By identifying business-critical systems, Purchasing Entities could duplicate these systems on AWS and have them always on.
- **Multi-Site Solution Deployed on AWS and On-Site:** A multisite solution runs in AWS and on a Purchasing Entities’ on-premises infrastructure in an active-active configuration. During a disaster situation, a Purchasing Entity can send all traffic to AWS servers, which can scale to handle its full production load.

Azure: Automating the replication of the VMs based on policies can protect Purchasing Entities’ environments that must achieve restoration within a four-hour period. Microsoft Azure offers Disaster Recovery as a Service where a Purchasing Entity automates the recovery of services in the event of a site outage at the primary data center. Purchasing Entities accomplish automated recovery services with the Site Recovery product. Site Recovery monitors the state of a Purchasing Entity’s protected instances. Replicating between two customer-controlled sites, including VMs and customer data, creates warm startup capability. All communication is encrypted. When replicating to Azure as the secondary site, Purchasing Entities select encryption for data at rest.

Site Recovery can protect Hyper-V, VMware and physical servers using the Azure secondary GovCloud data center as a recovery site. Site Recovery coordinates and manages the replication of data by integrating with existing technologies.

Autonomics ARC-P: The CSRA ARC-P solution can provide restoration of services within one hour of a severe outage at one of its data centers through continuous backups from our primary location to our Hot Stand-By location. ARC-P operates with a recovery point objective (RPO) of 60 minutes and an RTO of 60 minutes. For deployments on to other cloud services, CSRA cloud architects will help design a solution through our cloud migration services to meet the Purchasing Entity’s recovery and restoration goals.

6.8.1.5 Recovery Point Objective (RPO) and Recovery Time Objective (RTO) [8.8.1 (e)]

RPO and RTO goals can be achieved in multiple ways. One method to achieve RPO and RTO goals is to build the entire data center with a hot standby as CSRA has done with ARC-P. The CSRA ARC-P solution has an RPO of 60 minutes and a RTO of 60 minutes. The other method to achieve RPO and RTO goals is to build it into the design of the application deployment to the cloud. For deployment on to commercial cloud providers that do not guarantee RPO and RTO, CSRA cloud architects can work with the Purchasing Entity to design a solution to meet its needs through our cloud migration services.

6.8.2 Methodologies for Backup and Restore Services [8.8.2]

The backup and restore services differ per service offering in the CSRA solution, as described below.

6.8.2.1 Data Backups [8.8.2 (a)]

Based on the RTO and RPO requirements, CSRA will work with the Purchasing Entity to formulate a cloud model that meets the necessary requirements for data backups. We consider all capabilities in building high-availability environments with no single point of network or device failure. In addition, comprehensive backups protect the following infrastructure components:

- Server hardware and configuration
- Storage hardware and configuration
- Network hardware and configuration
- Virtual data center configuration

6.8.2.2 Server Image Backups [8.8.2 (b)]

VMs hosted in ARC-P can be configured with virtual disk snapshot schedules as shown in **Exhibit 6-11**. Virtual disk snapshots are automatically copied from cluster primary storage to zone secondary storage and replicated to the disaster recovery peer of the region. Individual files can be restored from snapshot by performing a 'Create virtual disk from snapshot' operation and attaching the virtual disk to a VM. Files can then be copied out of the virtual disk.

Recurring Snapshots

You can setup recurring snapshot schedules by selecting from the available options below and applying your policy preference

Schedule: ☒ Hourly ☐ Daily ☐ Weekly ☐ Monthly

Time: minute(s) Past the Hour

Timezone:

Keep: snapshot(s)

[Add](#)

Scheduled Snapshots

Time	Frequency	Timezone	Keep	Action
7:00	Every Day	US:Eastern [Eastern Standard Time]	7	✕
8:00	Every Sunday	US:Eastern [Eastern Standard Time]	4	✕
9:00	Day 1 of month	US:Eastern [Eastern Standard Time]	12	✕

[Done](#)

Exhibit 6-11. Virtual Disk Snapshot Schedule. Users can schedule hourly, daily, weekly, or monthly automatic virtual disk snapshots.

6.8.2.3 Digital Location of Backup Storage [8.8.2 (c)]

Digital location of backup storage depends of the level of service purchased. We offer local recovery to disk or tape at the primary data center, off-site archival to a third-party vendor, and multiple tiers of DR.

6.8.2.4 Alternate Data Center Strategies [8.8.2 (d)]

CSRA's cloud services have high-availability infrastructure components, including alternate data centers within the CONUS, redundant components, active-active and active-passive device pairing, load-balanced compute paths, redundant power supplies; backup power; and multipath network connectivity.

CSPs use different regions and availability zones which serve as alternate data centers for the primary hosting locations with continuous replication. ARC-P operates across two CONUS-only sites in an ACTIVE/HOT standby configuration; Ashburn, VA and Atlanta, GA. With the ACTIVE/HOT stand-by system in two separate data centers, the entire stack replicates every 15 minutes. If the system loses an entire data center, ARC-P can maintain normal operations without having to pull from a stored back up. ARC-P operates with an RPO of 60 minutes and an RTO of 60 minutes.

6.9 DATA PROTECTION [8.9]

All cloud vendors provide FIPS 140-2 compliant security encryption and cryptographic modules for protection of Participating or Purchasing Entities' data at rest and SSL/TLS encryption for Web modules provided by the vendors.

6.9.1 Standard Encryption Technologies and Options [8.9.1]

All cloud vendors provide FIPS 140-2 compliant security encryption and cryptographic modules for protection of Participating Entity's data at rest and SSL/TLS encryption for Web modules provided by the vendors. CSRA provides encryption technologies and options to protect sensitive data in transit or at rest as discussed in the following sections.

Data at Rest

Options for encrypting data at rest range from completely automated vendor encryption solutions to API-coded or manual, client-side options. Choosing the right solutions depends on the cloud services used and Purchasing Entity's requirements for encryption and key management. When considering encryption, Purchasing Entities have two primary choices:

1. Encrypt the underlying storage so all data gets encrypted automatically
2. Encrypt each piece of data as it's stored

From a usability perspective, the less need to worry about encryption for daily operations, the better. This usually leads to the encryption of the underlying storage. Encryption choices are:

- **AWS:** Amazon automatically encrypts data at the object level as it writes to disks in its data centers and decrypts it on access. AWS uses AES 128 and 256 bit encoding for default encryption and for customers with FIPS 140-2 requirements, SSL terminations in AWS GovCloud (US) operate using FIPS 140-2 validated cryptographic modules.
- **AWS Key Management:** AWS uses a key management service (KMS) to provide a centralized control of encryption keys. KMS presents a single view into all of the key usage by an organization. Purchasing Entities can create keys, implement key rotation, create usage policies, and enable logging from the AWS Management Console or use an API.
- **Microsoft Azure:** Microsoft Cloud offers a range of encryption capabilities from AES 128 bit up to AES-256, giving Purchasing Entities flexibility to choose the solution that best meets their needs. FIPS 140-2 data encryption is available from the BitLocker FIPS-compliant environment.
- **Microsoft Azure Key Management:** Azure Key Vault (AKV) helps safeguard cryptographic keys and secrets used by cloud applications and services. By using AKV, Purchasing Entities can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords) by using keys protected by hardware security modules (HSMs). For added assurance, clients can import or generate keys in HSMs. If a Purchasing Entity chooses to do this, Microsoft will process the keys in FIPS 140-2 Level 2 validated HSMs (hardware and firmware).
- **Autonomic Resources ARC-P:** ARC-P does not provide disk encryption services.
- **Autonomic Resources ARC-P Key Management:** ARC-P exposes the Intel AES-NI instruction set within instances to facilitate disk encryption with the guest OS of the instance. (Microsoft BitLocker, Linux dm-crypt/LUKS or equivalent software).

Data in Transit

Protecting data in transit involves protecting network traffic between clients and servers or network traffic among servers. Cloud provider services a Purchasing Entity purchases support Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. If a Purchasing Entity hosts a Web server in an IaaS, SaaS or PaaS instance, the Entity assumes responsibility for data in transit encryption. Use SSL/TLS for any HTTP traffic with a validate certificate from a trusted third party. If the deployment does not use HTTPS as a transport, we will find the encrypted equivalent for the protocol used. It is notable that there is little performance impact of an all encrypted communications channel.

- **AWS:** AWS protects data in transit with support for SSL/TLS in CloudFront, Amazon RDS, and elastic load balancing.
- **Microsoft Azure:** Azure uses industry-standard secure transport protocols such as IPsec and SSL/TLS between user devices and Microsoft data centers, and within data centers. With Azure Virtual Networks, Purchasing Entities can use the industry-standard IPsec protocol to encrypt traffic between corporate VPN gateways and Azure or among VMs located on Azure Virtual Networks. Microsoft Office 365 and other offered services follow industry cryptographic standards such as SSL/TLS and AES to protect the confidentiality and integrity of Purchasing Entities' data.
- **Autonomic Resources ARC-P:** Purchasing Entities use the ARC-P SecureGateway with multi-factor authentication (MFA), a FIPS 140-2 Level 2 validated device, for orchestration of cloud resources. With ARC-P Virtual Private Cloud (VPC) Purchasing Entities can use the IPsec protocol to encrypt traffic between physical corporate networks and virtual networks hosted in the cloud.

6.9.2 Willingness to Sign BAA [8.9.2]

CSRA would sign a BAA with Purchasing Entities and currently does so with customers such as the states of New York, Maryland and North Carolina where we deliver health care information services. CSRA also has contracts with the Federal Government that require BAAs. CSRA will work with each Purchasing Entity to satisfy data security requirements including new agreements specific to the Purchasing Entity's needs.

6.9.3 Offeror's Use of Data in Master Agreement [8.9.3]

CSRA will use customer data only for its intended use for the Participating or Purchasing Entity. CSRA will not use customer data for any other purpose than for customer needs. CSRA does not data mine customer's data unless the customer requires it and does not resell customer data for any purpose. CSRA, Microsoft, and Amazon have policies and procedures that employees must follow when dealing with customer data.

6.10 SERVICE LEVEL AGREEMENTS [8.10]

CSRA's SLAs are negotiable. CSRA will work with the Purchasing Entity to meet their needs. CSRA has flexibility with our ARC-P and ARCWRX offerings.

6.10.1 Description of SLAs Ability to be Negotiated [8.10.1]

CSRA's Service Level Agreements (SLAs) are negotiable. CSRA will work with the Purchasing Entity to meet their needs. CSRA has the greatest flexibility with the ARC-P and ARCWRX offerings, which are CSRA owned.

6.10.2 Sample Service Level Agreement (SLA) [8.10.2]

Response time SLAs assures all Purchasing Entities get reimbursed for 1/30th of their applicable monthly recurring charges for any calendar month in which CSRA fails to notify the Purchasing Entity or respond to events within the time frames outlined in the schedule below. We define the following terms for this SLA's purposes:

- “Notify”: CSRA will call back or respond electronically to the designated Purchasing Entity contact.
- “Respond”: CSRA will begin working on the problem or ticket item, e.g., by calling the Purchasing Entity back to clarify the issue or by starting the technical investigation.
- “Mean Time”: Arithmetic mean; we will average all occurrences for a severity level over a calendar month.

Service Levels for AWS/Azure – Purchasing Entities purchasing AWS or Azure services are entitled to the service levels described on their respective Websites. CSRA does not provide any SLAs or SLA credits other than those provided by these companies to customers.

We provide a sample of ITSM SLAs in [Exhibit 6-12](#).

Service Category & SLA Description	Descriptions	Performance Standard
Service Desk		
Average Speed to Answer (ASA)	Response Time for EMOC to answer	<60 Sec Avg
Status Update Frequency	EMOC Tickets updated daily	90%
Customer Satisfaction Rating	Mean of Survey Averages per Quarter	3.5 score on scale of 1 to 5
Incident Management		
Resolution Time	% of Incidents meeting the Hourly Target Duration for respective Severity level	90% for all
Severity 1	<4 Clk Hrs	
Severity 2	<8 Clk Hrs	
Severity 3	<16 Bus Hrs	
Severity 4	<24 Bus Hrs	
Incident Management		
Time for customer to be notified when non security incident is found	Error Rate for those occurring after 1 Hr	10%
Service Asset and Configuration Management		
Percent Accuracy of key fields for CIs in CMDB of level 2-3 systems - 20% minimum per month sample	% of fields per CI of audited sample having error; Monthly	5%
Hardware Assets Inventoried - Level 1-3 systems - minimum 10% monthly sample	Annual; 100% concurrence of audits done monthly	100%
Software Asset Inventoried - Level 2-3 systems - minimum 10% monthly sample	Annual; 100% concurrence of audits done monthly	100%
Change Management		
Percent of successful implemented changes - Level 2 and 3	% of successful changes	80%
Percent of changes resulting in an incident	% of changes resulting in an incident	10%
Percent of Emergency Changes	% of emergency changes	<20%
Percent of Backed Out Changes	% of backed out changes	<20%
Release and Deployment Management		
Successful release percentage - Major	% of successful releases	80%
Successful release percentage - Minor	% of successful releases	80%
Successful release percentage - Emergency	% of successful releases	80%
Availability Management		
Percentage of System Availability - Level 2-3 Systems	Total System Hrs	99.90%

Service Category & SLA Description	Descriptions	Performance Standard
Percentage of LAN Availability	by total LAN Hrs	99%
Capacity Management		
% of CPU utilization - Level 2 and 3 systems - Enterprise	Monthly; Avg % of CPU Utilization of CSRA L2/3 supported DHS systems; Enterprise view	80%
% of Disk utilization - Level 2 and 3 systems - Enterprise	Monthly; Avg % of Disk Utilization of CSRA L2/3 supported DHS systems; Enterprise view	80%
% of SAN utilization - Level 2 and 3 systems - Enterprise	Monthly; Avg % of SAN Utilization of CSRA L2/3 supported DHS systems; Enterprise view	80%
% of Network Bandwidth utilization	Monthly; Avg % of Bandwidth Utilization of CSRA supported DHS DC1 Network Switches for LAN/WAN; Enterprise view	80%
IT Service Continuity Management		
Monthly Backup Success Rate Average	Monthly; % of Backups Not Having a Client failure 2 days in a row	98%
% of funded clients having DR plan documented	Annual; DR Funded Clients	100%
% Successful System Recovery Testing	Annual; System Recovery Tests performed	90%
% Successful LAN Recovery Testing	Annual; DC1 LAN Recovery Tests performed	90%
% Audits and Reviews of DR Plans Completed	Annual; DR Funded Clients' Plans Reviewed	100%
DR Level 1 - No DR		
DR Level 2 - >=30 days	Annual; % Testing Recoverable w/in threshold	100%
DR Level 3 - within 30 days	Annual; % Testing Recoverable w/in threshold	100%
DR Level 4 - within 8 days	Annual; % Testing Recoverable w/in threshold	100%
DR Level 5 - within 24 Hrs	Annual; % Testing Recoverable w/in threshold	100%
DR Level 6 - within 8 Hrs	Annual; % Testing Recoverable w/in threshold	100%
DR Level 7 - within 4 Hrs	Annual; % Testing Recoverable w/in threshold	100%
DR Level 8 - Active, Active - Complete failover and near zero recovery time and recovery point	Annual; % Testing Recoverable w/in threshold	100%
Additional - Available for Use One year after Contract		
Information Security Management		
Security Intrusion Detection	% of Intrusion Detections Captured by IDS Sensors	95%
Security Intrusion Reporting and Compliance	% of "significant" Incidents reported within 1hr	95%
Access Termination	% of terminated employees with access removed	95%

Service Category & SLA Description	Descriptions	Performance Standard
Vulnerability Scan Compliance - Level 3	% of Level 3 systems having no “high” vulnerabilities listed or are within the Comply Date posted	95%
Certification and Accreditation Compliance	% of systems/apps having full C&A support from CSRA with unexpired ATO	95%
Virus Protection Management Compliance to Standard - Level 2 - Wintel	% of Level 2 CSRA supported Wintel servers having Antivirus signatures newer than 5 days	95%
Information Security Awareness Training Compliance	% of CSRA employees having received Security Awareness Training	95%

Exhibit 6-12. Sample SLA

6.11 DATA DISPOSAL [8.11]

CSRA provides specific data disposal procedures, policies and destruction confirmation processes. Our cloud vendors commit to the privacy of Purchasing Entity data and backed adoption of international code of practices for cloud privacy, ISO/IEC 27018. Third-party auditors independently verified enterprise cloud providers to ensure they align with the ISO 27018 code of practice for the protection of personally identifiable information in the public cloud. Adherence also ensures transparency about the return, transfer, and deletion of personal information stored in vendor data centers. Details include:

AWS: AWS provides Purchasing Entities with the ability to delete their data. However, AWS customers retain control, ownership, and management of their data.

AWS Storage Device Decommissioning: When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process designed to prevent customer data from exposure to unauthorized individuals. AWS uses the techniques detailed in Department of Defense (DoD) 5220.22-M (“National Industrial Security Program Operating Manual”) or NIST 800-88 (“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Microsoft Azure: Data destruction techniques vary depending on the type of data object being destroyed, whether it is a whole subscriptions, storage, VMs, or databases.

- **Subscriptions:** If a purchased subscription (like Office 365) has expired or gets terminated, all associated customer data is held for 90 days before it is deleted in order to recover from accidental subscription cancellation. In no more than 180 days after expiration or termination, Microsoft will disable the account and delete customer data. If a storage account gets terminated within an existing subscription (or when a subscription deletion has reached its timeout), the storage account is not deleted for another two weeks to prevent mistakes.
- **Storage:** Once a storage account is deleted, or when blob or table data is deleted outside the context of a storage account deletion, the sectors on disk become immediately available for reuse. How long before they are overwritten varies, depending on the fullness and activity rate on the server, but is rarely more than two days.
- **Virtual Machines:** Virtual machines are stored in Microsoft Azure Storage as blobs, so the deletion rules apply as explained above in Storage. The virtualization mechanism ensures that another customer cannot read the spot on the disk until the data gets written again, thus mitigating the threat of data leakage. When a new virtual disk is created for a VM, it will appear to the VM to be zeroed, however, the explicit zeroing of the data buffers occur when a portion of the virtual disk is read before it is written. If a VM instance is reinitialized in place, it’s the same as if it had moved to new hardware.
- **Azure SQL Storage:** Azure SQL Database deleted data is marked for deletion. If an entire database is deleted, it is the equivalent of deleting the database’s entire contents. The SQL Database

implementation ensures that user data never leaks by disallowing all access to the underlying storage except via the SQL Database API.

Microsoft Azure Storage Device Decommissioning: When a disk drive used for storage suffers a hardware failure, it is securely erased or destroyed before Microsoft returns it to the manufacturer for replacement or repair. All of the data on the drive is completely overwritten to ensure that the data cannot be recovered. When such devices are decommissioned, they are purged or destroyed according to NIST 800-88 Guidelines for Media Sanitation.

Autonomic Resources ARC-P: All data within the Purchasing Entity's VM remains under the c Purchasing Entity's control. It is the Purchasing Entity's responsibility to destroy their VM. Upon deleting the VM within the ARC-P console, all VM data is deleted.

ARC-P Storage Device Decommissioning: When a hard drive fails within the ARC-P storage system, the device is securely erased using the NIST 800-88 Guidelines for Media Sanitation and placed within a locked media destruction bin. The media destruction bin is located within the dedicated, private cage space that only cleared ARC-P personnel can access. All media within the media destruction bin is scheduled to be destroyed quarterly. Failed storage devices are never returned to the hardware manufacturer or vendor.

CSRA Data and Storage Device Decommissioning: CSRA disposes of all in-service and DR media per NIST 800-88. Media Sanitation requires media scheduled for destruction to be secured in a locked container in a secure location awaiting destruction. All media is destroyed per local site or data center standard operating procedure.

6.12 PERFORMANCE MEASURES AND REPORTING [8.12]

6.12.1 Reliability and Uptime Guarantee [8.12.1]

CSRA's ARC-P Community and Private Off-Premises clouds provide 99.9% uptime to those Purchasing Entities that require it out-of-the-box outside of scheduled maintenance windows. ARC-P achieves this by using two data centers geographically separated by more than 600 miles with diverse interconnect routes between them. ARC-P operates across the two sites in an ACTIVE/HOT STAND-BY configuration; Ashburn, VA and Atlanta, GA. With the ACTIVE/HOT STAND-BY system in two separate data centers, the entire stack replicates every 15 minutes. If the system loses an entire data center, ARC-P can maintain normal operations without having to pull from a stored back up. To achieve uptime beyond 99.9% ARC-P can provide Akamai services based on the desired uptime and application requirements. ARCWRX sits on top of ARC-P and inherits ARC-P's uptime capabilities.

For the other services in the CSRA solution, there is no guaranteed uptime but 99.9% availability can be achieved with the help from CSRA's cloud architects. One method would be to load balance the application requiring the high availability (HA) across two or more geographically diverse data centers. With CSRA as a cloud broker, the Purchasing Entity has an additional option of using two or more independent CSPs. A CSRA cloud architect can work with the Purchasing Entity to meet their HA requirements.

6.12.2 Standard Uptime Service and Related SLA Criteria [8.12.2]

CSRA's ARC-P provides 99.9% uptime service outside of scheduled maintenance windows. Our SLAs for ARC-P provide for an RPO of 60 minutes and an RTO of 60 minutes in the case of a drastic redundant failure. For our other services, CSRA's cloud architects will work with the Purchasing Entities to design a solution that meets their uptime requirements. CSRA will negotiate SLAs with the Purchasing Entities for its solutions.

6.12.3 Processes for Call/Contact Support [8.12.3]

CSRA has experience developing and refining contact-handling procedures and call flows for CSCC solutions. Customers calling the CSCC receive information available 24x7 through customized automated

call distributor (ACD) call flow menus that provide customers with options such as information access and the ability to speak with a live CSR. Requests for live assistance get placed in an ACD queue for best service routing (BSR) to the next available CSR. BSR monitors the status of CSRs and adjusts call processing appropriately. Our approach to customer service ensures Purchasing Entities can choose the delivery channel that suits them best. CSRs can also transfer or refer inquiries to the appropriate agency or authority for response as necessary.

CSRA leverages our existing Avaya technology that enables call-processing capacity to expand as service demand increases. Avaya, a leader in the telecommunications industry as shown in **Exhibit 6-13**, has products to meet all CSCC requirements without workarounds.

CSRA works with Purchasing Entities to design effective, call flows, and our management team works with customers on script development and maintenance. CSRA works with Purchasing Entities on call flow design, development, and maintenance of the information content and audio messages used for all automated voice response services, such as IVR, voice recognition, and text-to-speech services.

During CSCC operational hours in the IVR, the customer has the option to speak with a live CSR. If the customer selects this option, the call is placed into CSRA's Avaya ACD queue (supporting telephone and TDD/TTY calls) for routing to the next available CSR. The CSR provides a customer-approved greeting and asks how he or she may be of assistance. The ServiceNow system guides the CSR through the call with call flow scripting and active selection of the appropriate solution based on the customer's responses to the CSRs questions. This approach delivers consistency of content and information provided to the customer. The CSR then captures the data elements the customer requires during the interaction.

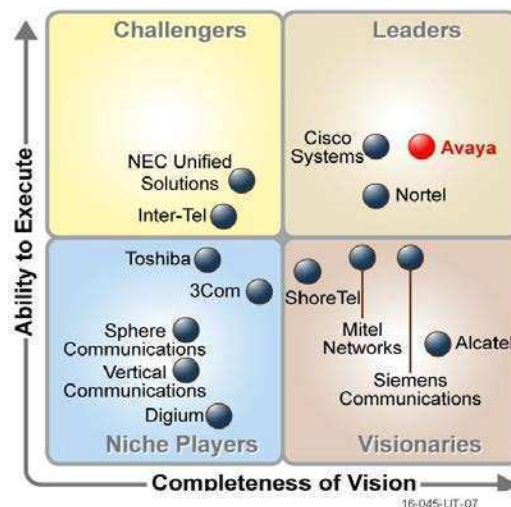


Exhibit 6-13. CSRA's Solution Set. Includes Industry-Leading Avaya Telecommunications.

CSRA follows best practices for these activities. The KM Service Delivery Life Cycle we use helps ensure the accuracy of the content within the knowledgebase and encourages information development and refinement through a communication style open to exchange, debate, discussion, resolution, and implementation. The KM Service Delivery Life Cycle process applies to content and scripts for all service delivery channels, including telephone, email and Web chat.

The KM Service Delivery Life Cycle process begins with the Identify and Develop Phase, where our KM Team's content research analysts (CRAs) collaborate with our clients to understand their requirements and develop the most appropriate scripts. Our KM Team gathers all available information; we then collaborate with our clients to develop a script that provides the information required to address the customer's concern. We use client-approved style guides to ensure that CSRs can effectively convey written scripts over the telephone.

We can conduct and complete the process for creating new scripts for rapid response and emergency situations. The CSRA KM Team's communication tools keep all CSRs informed with CSR roundtable meetings, which serve as focus groups to allow CSRs to express their concerns and suggestions regarding script changes. CSRA also provides a readily available question-and-answer line for CSRs to provide the KM Team with feedback and alerts about information that should be updated or added to ServiceNow.

Tier 1. Tier 1 support provides the initial contact point between the end user and a CSR via telephone, email, or voicemail. Tier 1 support provides end users with a flexible method to obtain support. Tier 1

team members receive training to respond to these requests and open tickets received from Tier 0. Tier 1 CSRs triage and resolve the majority of the issues the contact center receives and escalate issues they cannot resolve to Tier 2 via the CRM system.

On receipt of a call, Tier 1 CSRs create a ticket in the CRM system and use probing questions to understand the customer's concerns. They offer knowledge base information with standard resolution data for common problems that relate to customer applications, and they provide troubleshooting to remediate the caller's issue or referral information to other individuals or organizations. The knowledge base provides a library of common problem resolution actions accessible to all support staff.

Tier 2. Tier 2 support employees respond to issues beyond the expertise of the Tier 1 team. The Tier 2 staff typically provides support for complex application problems, troubleshooting of system issues, and escalating customers to SMEs. If the Tier 2 staff cannot resolve the problem, they escalate the ticket to Tier 3.

6.12.4 Consequences/SLA Remedies for Respondent Failures [8.12.4]

CSRA recommends an incentive/disincentive plan for meeting SLAs. The Purchasing Entity will not pay any amount over the invoices during the reporting period in this "no-cost," plan. The plan would operate with debits and credits on invoices. For any incentives, Purchasing Entities can forgive past missed credit. Disincentives will apply to either the invoice for the month the performance occurred or to the next month's invoice. We would negotiate this plan with the Purchasing Entity. We provide a sample of possible operating ranges for common SLAs in **Exhibit 6-14**.

SLA	Weight	Target Service Level	Minimum Service Level	Incentive	Operating Range (no incentive or disincentive)	Disincentive
Service Desk						
Speed to Answer	100%	95.00%	>92.00%	>95.00%	>92.00% to 95.00%	<=92.00%
Customer Satisfaction						
Customer Satisfaction Rating	100%	94.00%	>85.00%	>94.00%	>85.00% to 95.00%	<=85.00%
Incident Management						
Resolution Time (Severity 1, 2, and 3)	33.00%	99.00%	99.00%	Met 100% of category	Met 75.00% to <100 of category	Met <75.00% of category
Time for Customer to be notified when non-security incident is found	33.00%	90.00%	90.00%			
Status Update Frequency	33.00%	99.00%	99.00%			

Exhibit 6-14. Sample SLA Incentive Plan

6.12.5 Planned Downtime Procedures and Schedules [8.12.6]

Each of the services in the CSRA solution has different downtime procedures and schedules.

CSRA ARC-P / ARCWRX – ARC-P and ARCWRX operate under two set maintenance windows – Wednesday 6 p.m.-9 p.m. for changes that have no impact to the end user and uptime, and Saturday from 9 p.m.-3 a.m. for changes that may impact to the end user. The Saturday change windows are used as required for major changes one to two times per year. Change windows can be customized for private zone deployments and can run on a different schedule. However, when vulnerabilities are detected, we begin to immediately remediate the environment. Our objective aims to phase the remediation, using our built-in HA so virtual machines do not need to shut down, and the end user only experiences minor disruptions to portal access or network connectivity at most. We prioritize the infrastructure security

posture and the safety of Purchasing Entities' data, and depending on the severity of the threat, both could require unscheduled downtime.

Amazon AWS – Account administrators can see a calendar of scheduled maintenance in the console.

Microsoft Azure – Sends an email to the account administrators before scheduled maintenance.

Microsoft Office 365 – Account administrators can see a calendar of scheduled maintenance in the admin console.

Microsoft Dynamics – Sends an email to the account administrators five days before scheduled maintenance.

6.12.6 Consequences/Remedies for not Meeting Recovery Metrics [8.12.7]

CSRA recommends the same type of incentive/disincentive plan as for incident response SLAs discussed in Section 6.12.4.

6.12.7 Sample Performance Reports [8.12.8]

The IaaS offering in CSRA's solution provide Web-based performance reports with real-time statistics. We provide a sample of one from Microsoft Azure in **Exhibit 6-15**.

6.12.8 Printing Historical, Statistical and Usage Reports [8.12.9]

All the services in the CSRA solution allow Purchasing Entities to download historical, statistical, and usage reports to its local machine, at which point, they print the report on their printer.

6.12.9 24x365 On-Demand Deployment Support [8.12.10]

CSRA's Self-Service Portal leverages a FedRAMP-certified, SaaS deployment of the ServiceNow platform to provide the provisioning functionality the customer requires. ServiceNow, a leader in cloud-based service management solutions, is configurable and scalable. The Self-Service Portal will remain available 24/7 with a targeted up-time for the CSRA implementation of 99.9%, outside of scheduled downtime, which we will coordinate with the Purchasing Entity to minimize impact. Note that CSRA support staff will be available 24x7x365 to provide all the support necessary during any down time. CSRA's Self-Service Portal will enable customers to the provision cloud services in our solution.

6.12.10 Description of Scale-Up and Scale-Down Availability [8.12.11]

All the IaaS offerings in the CSRA solution have 24x365 scale-up and scale-down availability. CSRA also offers the Agility Cloud Management Platform (CMP), which allows for that scaling to complete automatically based on thresholds set by the Purchasing Entity. For example if the CPU utilization reaches 80% for two minutes on a Web server, it can automatically deploy another one. It will continue deploying additional Web servers if the threshold is breached until the maximum number of servers that the customer has configured in Agility is reached. Also, as the utilization falls below a set threshold, Agility can start shutting down servers to reduce cost.



Exhibit 6-15. Azure Performance Report Sample

6.13 CLOUD SECURITY ALLIANCE [8.13]

6.13.1 CSA STAR Self-Assessment [8.13 (a)]

The CSRA offerings of ARC-P, Amazon AWS, Microsoft Azure, Microsoft Office365 (which includes Skype for Business), Microsoft Dynamics, and ServiceNow have all completed the CSA STAR Registry Self-Assessment.

6.13.2 Completion of Exhibits 1 and 2 to Attachment B [8.13 (b)]

Service providers have completed exhibits 1 and 2 to attachment B, which are included in Volume 1 Attachments. The completed attachments include:

- Attachment 1: Amazon AWS CAIQ
- Attachment 2: CSRA ARC-P CAIQ
- Attachment 3: Microsoft Azure CAIQ
- Attachment 4: Microsoft Azure CCM
- Attachment 5: Microsoft Dynamics CCM
- Attachment 6: Microsoft Office 365 CCM
- Attachment 7: ServiceNow CCM

6.13.3 CSA STAR Registry Attestation, Certification of Assessment [8.13 (c)]

None of the CSRA offerings have a current CSA STAR Attestation, Certification, or Assessment.

6.13.4 CSA STAR Continuous Monitoring [8.13 (d)]

None of the CSRA offerings have current completed the CSA STAR Continuous Monitoring.

6.14 SERVICE PROVISIONING [8.14]

6.14.1 Processing Emergency or Rush Services Implementation Requests [8.14.1]

CSRA's solution uses the ServiceNow portal for provisioning services. As soon as the Purchasing Entity's accounts are created, it can provision services 24x365. Only initial deployments of dedicated private clouds require longer lead times as discussed in the next section. For any given emergency, the Purchasing Entity can deploy services without notice. CSRA's solution also contains auto-scaling capabilities for IaaS offerings, which allows Purchasing Entities to set up scripts to automatically deploy additional servers when utilization reaches a configurable threshold for a configurable amount of time.

6.14.2 Standard Lead-Time for Provisioning the Solution [8.14.2]

All the public, community, and virtual private cloud services in CSRA's solution are operational today with active users. Once an agreement is signed with a Purchasing Entity and accounts are created in our ServiceNow Portal, the Purchasing Entity can immediately start provisioning services. The dedicated on and off premises private ARC-P clouds will require additional time. The off premises ARC-P cloud will require several weeks to install and configure the hardware for the Purchasing Entity before they can provision servers on it. The lead-time for an on-premises ARC-P deployment depends on the breadth and depth of the requirement. An on-premises ARC-P zone would require a physical site security assessment, ARC-P zone deployment, and management software configuration and deployment. More information regarding the full requirements would be needed before a complete timeline can be established. The main impacts to the timeline would be the Purchasing Entity's security assessment requirements, initial deployment sizing, and initial functionality requirements.

6.15 BACK UP AND DISASTER PLAN [8.15]

Cloud computing, based on virtualization, takes a different approach to DR. Since the virtual server hardware is independent, the operating system, applications, patches and data can be safely transferred from one data center to a second data center without the burden of reloading each component of the server. This can dramatically reduce recovery times compared with conventional DR approaches. The cloud shifts the DR tradeoff curve. With a cloud provider, DR becomes more cost-effective with faster recovery times.

6.15.1 Legal Retention Periods and Disposition [8.15.1]

Retention and disposition is a plan that indicates the period of time a Purchasing Entity should retain records. Records schedules allow for disposing of records in a timely, systematic manner by setting retention and disposal guidelines based on administrative, legal, fiscal, or research needs. Each of our cloud vendors has set specific guidelines for data retention. These are similar across all vendors. If data is to be retained for record purposes past the retention policies of the vendor, each Purchasing Entity will need to manage their data and its disposition according to their retention policies.

AWS: Maximum retention period for automated backup is 35 days.

Microsoft Azure: Microsoft will retain Purchasing Entity data stored in the online service in a limited function account for 90 days after expiration or termination of subscription. After the 90-day retention period ends, Microsoft will disable a customer's account and delete the customer data. The online service may not support retention or extraction of software provided by the Purchasing Entity. Microsoft has no liability for the deletion of customer data.

Autonomic Resources ARC-P: All data within the customer VM is under the customer's control. Purchasing Entities can deploy data archiving methods within their virtual environment to retain data separately from active VMs. Purchasing Entities can have user access removed at any time 24x7x365 for production systems. Purchasing Entities can have their VMs, data disks or archival storage retained for a customer-defined period of time to facilitate data retention needs.

CSRA: CSRA stores no user data for Purchasing Entities.

6.15.2 Inherent Disaster Recovery Risks and Potential Mitigations [8.15.2]

When hardware or software fails within a cloud environment, the techniques and strategies for managing them differ than when failure occurs in on premise data centers. Cloud solutions typically have more dependencies on infrastructure that is dispersed across the data center and managed as separate services. To deal with service failures, Purchasing Entities must deal with partial failures using high-availability techniques. To manage more severe failures, Purchasing Entities must think and use DR strategies.

Cloud vendors detect and handle many failures, but many types of failures require application-specific strategies. Purchasing Entities must prepare for and manage the failures of applications, services, and data. When creating an application availability and DR plan, Purchasing Entities must consider the business consequences of the application's failure. Once business continuity plans are established, they must be regularly analyzed, tested, and improved based on the application portfolio, business needs, and the technologies available. Cloud vendors continually provide new capabilities and challenges to creating applications that withstand failures.

6.15.3 Infrastructure Supporting Multiple Data Centers [8.15.3]

CSRA cloud solutions vendors have designed solutions to support strategic scenarios that require speed, scale, security, compliance and economics for government organizations. All our vendor solutions meet the higher level security and compliance needs for sensitive, dedicated, US Public Sector workloads found in regulations such as FedRAMP, DoD Enterprise Cloud Service Broker (ECSB), Criminal Justice Information Services (CJIS) Security Policy and the Health Insurance Portability and Accountability Act (HIPAA).

AWS: AWS provides Purchasing Entities with the flexibility to place instances and store data within geographic regions and across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. The four regions are: US East (Northern Virginia), US West (Oregon), US West (Northern California) and AWS GovCloud (US). AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move workloads into the cloud by helping them meet regulatory and compliance requirements. The AWS GovCloud (US) framework allows US government agencies and their contractors to comply with US International Traffic in Arms Regulations (ITAR) regulations as well as the FedRAMP requirements. AWS GovCloud (US) has received an agency ATO from the US Department of Health and Human Services (HHS) using a FedRAMP-accredited Third Party Assessment Organization (3PAO) for AWS services.

Microsoft Azure: The Azure government environment is a separate instance from Microsoft Azure public and only used by qualified US government organizations and solution providers. The Azure government environment maintains two data centers over 500 miles apart. All customer-managed data is stored within the CONUS data centers. All Azure government operators and administrators are screened US citizens.

Autonomic Resources ARC-P: ARC-P operates across two CONUS sites in an ACTIVE/HOT STAND-BY configuration: Ashburn, VA and Atlanta, GA. With the ACTIVE/HOT STAND-BY system in two separate data centers, the entire stack replicates every 15 minutes. If the system loses an entire data center, ARC-P can maintain normal operations without having to pull from a stored back up.

CSRA: CSRA operates a dual data center model with the primary data center in Bossier City, LA and the secondary data center in Raleigh, NC.

6.16 SOLUTION ADMINISTRATION [8.16]

Each Purchasing Entity will collect mechanisms and procedures that permit system managers to exercise or restrain behavior and content of their systems within the cloud. Cloud technology has the power to shift competitive landscapes by providing a platform for creating and delivering business value. Purchasing Entities need to determine cloud-enabled business models that promote sustainable cost advantage to take advantage of cloud's potential to transform internal operations.

6.16.1 Managing Identity and User Accounts [8.16.1]

Responsibility for the security of information and information systems belongs to the Purchasing Entities who purchase capability from the cloud providers. Each vendor provides tools that Purchasing Entities may use to provision resources and access cloud instances and data, but it is the Purchasing Entity who grants access to users. In addition to the authentication mechanism (such as a password), access control is concerned with how authorizations are structured. In some cases, authorization may mirror the structure of the organization, while in others it may be based on the sensitivity level of the documents and the clearance level of the user accessing those documents. The Purchasing Entity has responsibility for authentication and authorization. We describe IAM capabilities for each vendor below.

AWS: AWS's Identity and Access Management (IAM) enables customers to control access to AWS services and resources. Using AWS IAM, Purchasing Entities create and manage AWS users, groups, and use permissions to allow and deny access to customer AWS resources. AWS Identity and Access Management (IAM) let customers manage long-term security credentials for IAM users:

- **Passwords:** Used to sign in to secure AWS pages, such as the AWS Management Console and the AWS Discussion Forums.
- **Access keys:** Used to make programmatic calls to AWS from the AWS APIs, AWS CLI, AWS SDKs, or AWS Tools for Windows PowerShell.
- **Amazon CloudFront key pairs:** Used to create signed URLs for the CloudFront product.
- **SSH public keys:** Used to authenticate to AWS CodeCommit repositories.
- **X.509 certificates:** Used to make secure SOAP-protocol requests to some AWS services.

In addition to managing user credentials, security can be enhanced through the use of multi-factor authentication.

Microsoft Azure: Microsoft offers two solutions for the management of cloud access management, Microsoft Azure IAM Cloud and Microsoft Identity Access manager. IAM Cloud is a cloud specific identity management platform wholly hosted on Microsoft Azure. IAM Cloud is offered as a service, with a full customer success program included within the price to ensure customers are fully supported throughout onboarding and day-to-day use including configuration changes and adding new applications. Microsoft Identity Manager is an on premise identity and access management product that centrally manages identities across data centers and the cloud, providing secure single sign-on to applications in the hybrid cloud environment. Microsoft Identity Manager provides identity management through Windows Server Active Directory and Forefront Identity Manager. This product provides Purchasing Entities a set of cloud-based identity and access management solutions on Azure Active Directory.

Autonomics ARC-P: The Purchasing Entity assumes responsibility for all users with access to provision within ARC-P IaaS and ARCWRX PaaS and for granting access to connect to the virtual machines running within either platform.

CSRA: CSRA's Agility Platform provisions cloud instances from the cloud vendors for Purchasing Entities. Customer selection of a cloud vendor and vendor capabilities is based on the authority of a ServiceNow user and their privilege to select items from the ServiceNow catalog. Agility Platform policies govern which applications and instance types can be placed in the different cloud environments, including which users and groups are authorized to create an instance. These policies dictate which workloads can be deployed to authorized cloud environments.

6.16.2 Providing Anti-Virus Protection [8.16.2]

Purchasing Entities may provide Anti-virus end point protection or may purchase it from a cloud vendor or CSRA.

AWS: AWS offers partners who offer anti-virus tools and features to help customers meet security objectives around visibility, auditability, controllability and agility.

Microsoft Azure: Microsoft Endpoint Protection for Windows Azure provides the ability to include an anti-malware protection agent in each Windows Azure virtual machine running Windows Azure service. Microsoft Endpoint Protection for Windows Azure supports Windows 7 Home Premium 64-bit, Windows 7 Professional 64-bit, Windows 7 Ultimate 64-bit, Windows Server 2008 R2 SP1, Windows Server 2008 Service Pack 2 and Windows Azure SDK 1.7.

Autonomics ARC-P: The ARC-P IaaS provides Sophos antivirus for centralized antivirus detection and management.

CSRA: CSRA offers a comprehensive set of cyber security services for Purchasing Entities that provide the flexibility of purchasing these services from CSRA or to use their own personnel on premise with security products hosted by CSRA. We provide CSRA security tools from our NOSC. This flexibility allows Purchasing Entities who are still uncomfortable with “outsourcing” their security to start by using on premise resources and as they build confidence and trust with security capabilities. Purchasing Entities may migrate to a managed security service over time. Either way, CSRA will deliver world-class security capabilities to federal and state clients.

Our Server and Endpoint Security offering provides the capability to protect endpoints by whitelisting binaries and processes. It dynamically prevents unapproved applications, process, and binaries from executing. This provides a non-signature based approach for preventing malware from executing (including zero day exploits). If the service is purchased from CSRA, we will monitor the customers cloud instance(s) from our NOSC. The endpoint service is built on Carbon Black.

Key features of Carbon Black include:

- Real-Time Visibility on Every Endpoint & Server
 - Unmatched Advanced Threat Prevention
 - Default Deny
 - Detect and Deny
 - Detonate and Deny
- Signature-less Detection
- Rapid Response with Full Kill Chain Analysis
- Open API for Seamless Integration with Existing Security Tool Sets
- Broad Platform Support (Windows, Mac, Linux)
- Enterprise Ready, Scalable, Reliable

6.16.3 Migrating Data, Metadata and Usage Data [8.16.3]

Purchasing Entity’s data is owned and controlled by them. The Purchasing Entity may at any point download, transfer or delete their data on CSRA’s solution. However, Metadata is not retrievable or extractable, and may not be deleted, by Purchasing Entities. It is stored in internal databases, and retained and protected by the service providers. Before decommissioning a system or account, the Purchasing Entity should ensure the any data that they require is transferred to another system, cloud provider or their own data center. For large amounts of data that need to be transferred, where moving the data over a network would be prohibitively long and expensive, some of our solutions have the option to put the data on to a hard drive and mail it to the Purchasing Entity. For this option, the data is encrypted before being places on the hard drive to ensure the security of the data in transit. The encryption keys are provided separately to the Purchasing Entity.

CSRA has cloud migration services that the Purchasing Entity can use not only migrate onto a cloud from our solution, but also from our cloud to another cloud provider. In both cases, this service is provided at a fixed cost to the Purchasing Entity to provide a very predictable cost model.

6.16.4 Administering the Solution in a Distributed Manner [8.16.4]

CSRA's solution is comprised of cloud services, which by definition are location-agnostic. So long as users from the Purchasing Entities have Internet connectivity and the required accounts on our system, they will be able to administer the solution. These users can be spread across the US and do not have to be collocated in a single facility.

6.16.5 Applying Defined Administration Policies [8.16.5]

If the Purchasing Entities needs to apply their administration policies to the cloud solutions, CSRA's Agility Platform should be selected. It can provide the ability to set custom governance policies to the cloud services. This includes the ability to create custom policies based on an extensible meta-model, enabling consumption resources based on custom parameters. The Agility Platform:

- Converts rules, decisions, and rights for the usage of IT resources into policies
- Ensures that cloud resource accessibility, provisioning, security, and operating procedures are executed in accordance with policies
- Provides automatic alerting mechanisms and remediation responses if policies are violated
- Provides capabilities to track policy changes and generate audit trails

6.17 HOSTING AND PROVISIONING [8.17]

6.17.1 Cloud Hosting Provisioning Processes and Provisioning Stack [8.17.1]

CSRA's Self-Service Portal leverages a FedRAMP certified, SaaS deployment of the ServiceNow platform to provide the provisioning functionality the customer requires. CSRA's ServiceNow-based portal will provide Purchasing Entities the interface to provision all of the offerings in CSRA's solution. Most of the offerings will be immediately provisioned/de-provisioned, such as virtual machines, software as a service accounts, and storage. Selection of some of the offering will open a trouble ticket with the CSRA help desk to request further information and coordination. Examples of these types of offerings are dedicated on or off premises private clouds.

For the automated provisioning tasks, ServiceNow will interface with the CSRA Agility CMP. Agility will then ensure that the correct service is provisioned on the correct service provider.

6.17.2 Providing Tool Sets [8.17.2]

CSRA's primary provisioning tool is ServiceNow and monitoring tools are those native to the cloud offerings. Amazon has CloudWatch, Microsoft has it built into their portal and CSRA's ARC-P has CloudForms. CSRA offers the Agility Platform for added capabilities described below. CSRA also offers Application Performance Monitoring (APM), a software class designed to monitor the performance and availability of complex software. CSRA's APM offering revolves around three APM products in the market: Dynatrace, AppDynamics, and New Relic. More detail on APM product is provided below.

6.17.2.1 Deploying New Servers [8.17.2.1]

Through ServiceNow Purchasing Entities will be able to deploy new servers in any of CSRA's Infrastructure as-a-Service offerings. These servers also can be deployed as stand-alone servers. Purchasing Entities can create a server farm from stand-alone servers by placing a virtual load balancer on the network in front of the servers and configuring the balancing rules appropriately. New servers can be deployed to existing server farms by modifying the customer's virtual load balancer rules.

6.17.2.2 Creating and Storing Server Images [8.17.2.2]

All of CSRA's IaaS offerings allow Purchasing Entities to create and store server images they can use for deployments. This capability is native to these services. In addition to that, Agility's Designer module enables CSRA to assemble everything from simple stacks to multitier application blueprints and topologies, and enables these workloads to have the cloud portability that Purchasing Entities need for vendor contestability, combined with the business agility provided by on-demand provisioning. Using Agility Designer, customer workloads such as development platforms, custom business applications, and packaged applications are assembled into blueprints and outfitted with application configuration controls,

auto-scaling rules, storage tiers, security settings, governance controls, and embedded with operating environment agents and utilities. Agility Designer allows CSRA to construct for Purchasing Entities a policy-compliant and portable “everything as a service” portfolio that is policy-compliant and portable across heterogeneous cloud types in the CSRA solution. When these cloud workloads are assembled, they can be promoted to the next lifecycle stage for publishing and end-user consumption.

6.17.2.3 Securing Additional Storage Space [8.17.2.3]

CSRA’s ServiceNow platform will allow Purchasing Entities to provision additional storage space in any of the cloud environments in CSRA’s solution.

6.17.2.4 Monitoring Tool Use [8.17.2.4]

All of CSRA’s IaaS offerings have built in monitoring capabilities for public and hybrid clouds that allow the Purchasing Entities to see their CPU, Disk I/O, Memory, and Network I/O usage on given cloud provider. If the Purchasing Entity needs additional capabilities, the CSRA Agility Platform’s Operations module simplifies IT operations management functions across the heterogeneous private and public cloud environments. It consolidates monitoring, reporting and benchmarking capabilities. The Operations module abstracts the technical and operational differences between the cloud providers in CSRA’s solution for uniform visibility into resource consumption, performance, costs, availability, and other metrics. Purchasing Entities can compare cloud provider performance across different operational parameters and limits, such as average VM provisioning time, number of failed or degraded instances, and max number of concurrent provisioning requests executed.

Dynatrace: For the Purchasing Entities that require deep-dive analytics into the underlying code and rapid root cause analysis at levels no other APM tool can reach, CSRA offers an APM offering powered by Dynatrace. This offering provides immediate run-time visibility into application health, quickly maneuvering between high level heuristics to RPC calls with ease. This robust performance evaluation engine provides complete access to the level of granularity required to root out the most challenging of application performance issues. We consider this offering our bottoms-up approach to performance analysis, measuring at the lowest level and adding layers to achieve the complete picture.

AppDynamics: AppDynamics APM capability offers granularity to visualize and prioritize the end-to-end business transactions performance, and the health of the application and infrastructure nodes. We consider this our on-premises top down approach to performance analysis providing the right level of access to the right amount of performance data to make automated or analytical based decisions proactively against operational environment.

New Relic: New Relic’s SaaS-only model simplifies product installation by obviating the need to provision a collector server and dashboard. Rich metrics are available in a Web-based dashboard immediately after agents and JavaScript are instrumented in the application and on the servers. New Relic provides monitoring and deep inspection into infrastructure, web transactions, application availability, and application performance. These capabilities provided valuable and immediate feedback to developers and testers as they worked in short intervals to develop new features, fix bugs and regressions, and conduct load tests to measure system capacity. We consider New Relic the APM option of choice for Purchasing Entities that embrace a SaaS-based model.

6.18 TRIAL AND TESTING PERIODS (PRE - AND POST - PURCHASE) [8.18]

6.18.1 Testing and Training Periods for Offerings [8.18.1]

CSRA offers free and billable training and testing options to Participating or Purchasing Entities. CSRA provides free Web-based training on its portal; and vendors of the solutions in CSRA’s catalog also provide free training as well as trial periods, which vary from solution to solution.

6.18.2 Providing Test and/or Proof of Concept Environment [8.18.2]

At the request of a Participating or Purchasing Entity, CSRA will perform a live demonstration of the solution. If longer testing is required, we will build a paid proof of concept environment that allows

customers to evaluate requested features. The proof of concept can include any services offered in this proposal.

6.18.3 No-Cost Training and Support Provided by Offeror [8.18.3]

We provide basic training and support at no additional cost to Participating Entities. Web-based training is available from CSRA's service catalog and through vendors. Advanced training is available for an additional cost; and we collaborate with Participating Entities to determine its scope, audience and format are developed. An estimated cost is developed based on requirements, and presented to the Participating Entity for approval.

Basic help desk support is available at no additional cost to the customer. This service includes account management and incident support. If additional support services are needed, CSRA guides the Participating Entity to the appropriate service in our catalog or builds an estimate to provide the services if unavailable in the catalog. As a large systems integrator, we can provide the level of support needed, from simple patch management to complex data center migrations to the cloud. CSRA has provided this range of support to US, State and Local government agencies, including the State of California DHS, and FAA, for many years.

6.19 INTEGRATION AND CUSTOMIZATION [8.19]

CSRA offers a range of integration and customization options to the Participating or Purchasing Entities. We detail these options below.

6.19.1 Integration of Services into Complementary Applications [8.19.1]

CSRA's cloud services solution supports the largest number of APIs and third-party products in the market via the CSRA Agility Platform. Purchasing Entities developing application blueprints from within Agility Designer would have the ability to pull in virtual appliances of products and graphically configure their stacks similar to a drag-and-drop, snap-to-grid interface such as Microsoft Visio. If product connectors are not available out-of-the-box, Agility offers a REST API that leverages the Open Grid Forum's Open Cloud Computing Interface Core Model specification with an extensible meta model. Through the REST API, all Agility module features remain accessible, allowing for minimal code requirements to enable desired functionality.

The Agility Platform SDK enables Purchasing Entities to build their own cloud adapters to govern and control IT resource managers, including bare-metal provisioning tools.

Agility Platform provides an intuitive command line interface that enables rapid DevOps toolchain integration. In addition, technical users can use the CLI to instruct the Agility Platform to execute a range of commands and functions from the convenience of a command line tool rather than through the Agility Platform graphical Web interface.

Purchasing Entities can use Agility Platform's API to access governed enterprise cloud services from IT products and tools; including developer tools, continuous software build tools, third-party portals, and IT ops dashboards. Every capability exposed via Agility Platform's full-featured API goes through the same policy-driven IT governance and security controls. Furthermore, Agility's third party connectors will enable rapid extensibility to the governance, management, configuration and security workflows to other systems. This capability provides Purchasing Entities with the assurance that best-in-class tools can be incorporated into their enterprise architecture as their needs evolve, yet investments in existing products can continue to produce value.

6.19.2 Customization and Personalization of Services [8.19.2]

By its nature, Infrastructure as a Service (IaaS) is highly customizable. Purchasing Entities can install a variety of operating systems and applications with IaaS. Applications can be custom-developed or commercially available products. With available load balancers, Purchasing Entities can build high performing available systems.

CSRA's PaaS allows the Purchasing Entities to build custom application without the expense of maintaining their development environments. CSRA's PaaS offering provides preconfigured, pre-integrated agile application lifecycle management platform designed to shorten the time to value, reduce acquisition and maintenance costs and allow Purchasing Entities to focus on application development and not the creation and maintenance of the required engineering environments and tools.

These may be true of many IaaS or PaaS providers, but CSRA brings additional capabilities with the Agility Platform. With the Agility CMP, CSRA can provide broker services between existing virtualized environments, community clouds, public clouds, and private clouds. This would allow the Purchasing Entities to maintain investments already made in existing hardware and tie into one seamless interface. Through the Agility Platform, Purchasing Entities can manage true hybrid cloud environments from one single interface.

Agility's Release Manager allows customization of the Purchasing Entity software lifecycle stages to reflect each group's SDLC and establish role-based permissions to promote, accept and approve software builds at each stage. With Release Manager, the Purchasing Entity can leverage policies and enable release automation across stages, or introduce manual release approval processes with integration into the Purchasing Entity's existing SDLC tool chains and approval workflows. Release Manager accelerates the Purchasing Entity initiatives for DevOps, and continuous delivery and integration. The Release Manager provides the Purchasing Entity additional capabilities and benefits to include: on-demand platform provisioning with embedded standard operating environments; automated application and service configuration; and management of security and operational SLAs across each role in the SDLC. Agility Release Manager leverages these high-fidelity runtime environments across the lifecycle and achieves significant cycle time.

6.20 MARKETING PLAN [8.20]

Sales leadership in SaaS, PaaS, IaaS, and other cloud products and services is one of CSRA's top priorities. Our organizational structure features a cloud technology brand manager charged with researching market trends, identifying and recommending key technologies, and educating our customers and our internal account teams on cloud technology. Our cloud brand manager works with our Contract Manager and our State and Local government account teams to support general marketing, increase our presence at trade events, and provide in-person expertise to customer visits, consultations, and demonstrations.

Our investments in our cloud offerings have generated SaaS, PaaS, and IaaS business solutions that can be directly applied to NASPO ValuePoint Cloud Solutions procurement opportunities. Our Marketing action plan extends these capabilities, as shown in **Exhibit 6-16**, to meet our clients' requirements. Specifically for NASPO, our Contract Manager maintains the plan, tracks progress, and enforces accountability against a formal plan. In each area, initial actions will be completed within 30 days of contract award; steady state marketing operations will be achieved within 90 days.

Area	Assets and Resources in Place	Actions	Responsibility
Staff awareness and training	- Technical staff aware and trained (SaaS, IaaS, PaaS) - Business developers aware and trained (IaaS, PaaS)	- Brief account teams and product teams about NASPO vehicle and its advantages - Schedule presentations and other refresh activities (e.g., quarterly teleconferences) - Publicize early opportunities, successes	- Contracting Officer - State & Local VPs
Build NASPO	- Roster of IaaS, PaaS and IaaS opportunities - Account plans and call plans for states	Meet with responsible business developers to	Contracting Officer

Area	Assets and Resources in Place	Actions	Responsibility
vehicle new business pipeline	- Advertising, social media and email campaigns - Joint pipeline reviews with alliance partners	- promote NASPO vehicle as a contracting option - Attend account planning meetings, review/refine account plans to verify consideration of NASPO vehicle - Attend sales calls (supporting role)	- State & Local VPs - Account teams
Marketing support	- Infographics, white papers “Event in a Box” for sharing SaaS, IaaS and PaaS info - Webinar series - Success stories (video, text) - Attend conferences (NASCIO, MESC, etc.)	- Develop simple guides to provide NASPO vehicle details (hardcopy, online) - Develop customer training materials - Identify, obtain, and distribute model RFPs for use by OCOs - Integrate NASPO vehicle into corporate marketing campaign	- Contracting Officer - State & Local VPs - IaaS, PaaS and IaaS product offering managers - Marketing team
Contract marketing	- GWAC Center of Excellence (COE) awareness - Presence at major state government conferences (i.e. NASCIO)	- Develop NASPO vehicle web site - Attend conferences and events - Update all GWAC COE systems and materials to include NASPO vehicle	- Contracting Officer - State & Local VPs
Streamlined proposal process	- SaaS, PaaS and IaaS product definitions and pricing - Templates for startup/ transition	- Tailor or refine existing methods for NASPO vehicle needs - Prepare reusable proposal artifacts	- Contracting Officer - Proposal director

Exhibit 6-16. Marketing Action Plan. Our Marketing action plan defines actions and responsibilities to drive business to the NASPO vehicle.

6.21 RELATED VALUE-ADDED SERVICES [8.21]

CSRA offers cloud migration services, APM, and patch management. We have refined our process to the point that we can offer migration services as fixed-price options. As a result, the customer will always know how much it will cost to migrate its environment to the cloud.

CSRA offers APM, a software class, designed to monitor the performance and availability of complex software. CSRA’s patch management process breaks down into the following four processes as depicted in [Exhibit 6-17](#) with tasks assigned to each phase:

- Assess
- Identify
- Evaluate and Plan
- Deploy

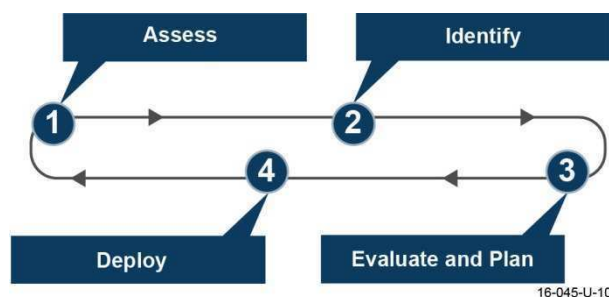


Exhibit 6-17. Patch Management Phase Workflow

Assessment phase

- Determine what is currently in the production environment
- Evaluate security threats and vulnerabilities
- Prepare to respond to new software updates

Identification phase

- Discover new software updates/patches/hot fix in a reliable way
- Determine whether an update is relevant to our production environment
- Determine the deployment classification for an update

Evaluation and planning phase

- Make a go/no-go decision to deploy a software update/patches/hot fix
- Determine what is needed to deploy an update
- Test the software update/patches/hot fix in a test environment to confirm that it does not compromise business-critical systems and applications
- Gain approval for deployment

Deploy phase

- Roll out the approved software update/patches/hot fix into our production environment
- Meet all of the requirements of any deployment SLAs
- Update baselines in preparation for the next process cycle

6.22 SUPPORTING INFRASTRUCTURE [8.22]

CSRA's supporting infrastructure requirements are provided in the subsections below.

6.22.1 Required Infrastructure [8.22.1]

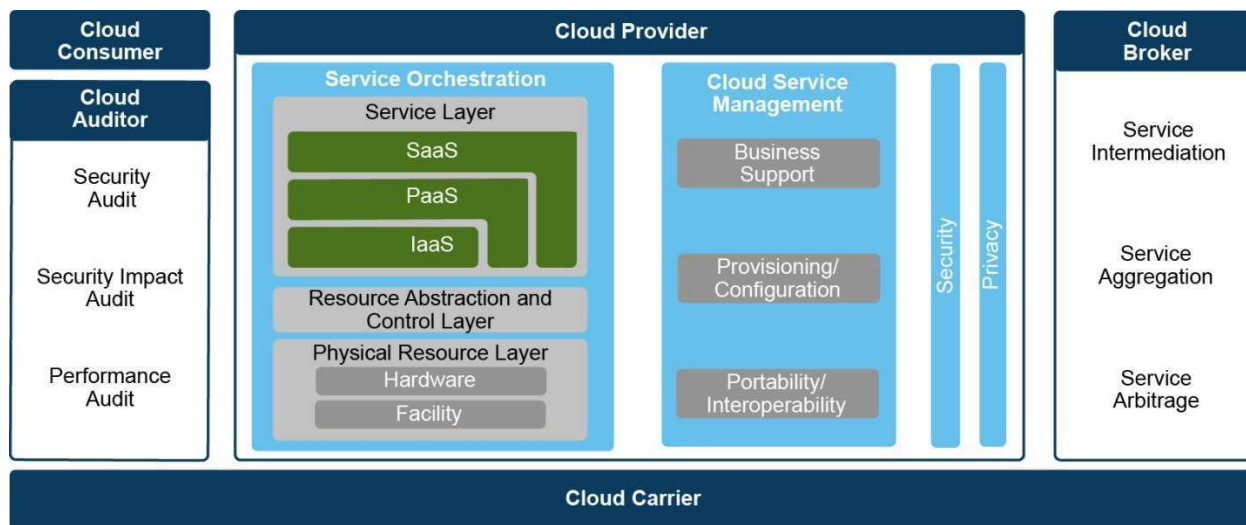
The Purchasing Entity does not require any additional infrastructure to support the services and deployment models CSRA offers with the exception of the on-premises ARC-P IaaS cloud. For the deployment of on-premises solutions, the Purchasing Entity must provide power, heating and cooling, rack space, and network connectivity within its data center. In addition, the Purchasing Entity will be required to pay for the purchase of infrastructure for deployment, a gap assessment of the agency premise to bring the site within the ARC-P ATO security boundary, and a small assessment by a 3PAO.

6.22.2 Responsibility for Installation of Infrastructure [8.22.2]

For the on-Premises ARC-P infrastructure as a service cloud, CSRA will assume responsibility for the installation. The Purchasing Entity assumes responsibility for the cost, which we list in our services catalog.

6.23 ALIGNMENT OF CLOUD COMPUTING REFERENCE ARCHITECTURE [8.23]

CSRA's architecture compares closely to the NIST Cloud Computing Reference Architecture depicted in **Exhibit 6-18**. CSRA offers services from industry-leading IaaS, PaaS, and SaaS providers.



16-045-U-15

Exhibit 6-18. The Conceptual Reference Model from the “NIST Cloud Computing Reference Architecture”

We provide service intermediation, aggregation, and arbitrage through our ServiceNow Cloud Portal and Agility CMP. The services we offer are listed in [Exhibit 6-19](#) and align with the NIST definitions of the IaaS, PaaS, or SaaS domains.

Name	NIST Service Model Domains
Amazon AWS	IaaS
CSRA ARC-P	IaaS
Microsoft Azure	IaaS
AppWorks	PaaS
ARCWRX	PaaS
Office 365	SaaS
Microsoft Dynamics CRM Online	SaaS
ServiceNow	SaaS

Exhibit 6-19. Service Model Domains for CSRA Offerings

Section 7: Confidential, Protected or Proprietary Information [3.12.7]

None

State of New Jersey Compliance Terms and Conditions

The following terms and conditions shall be deemed incorporated by reference into each Participating Addendum entered into by the State of New Jersey under an awarded Master Agreement. The State of New Jersey reserves the right to add additional terms and conditions to each Participating Addendum.

1. LAW REQUIRING MANDATORY COMPLIANCE BY ALL CONTRACTORS -

The statutes, laws or codes cited herein are available for review at the New Jersey State Library, 185 West State Street, Trenton, New Jersey 08625. The contractor must comply with all local, State and Federal laws, rules and regulations applicable to this contract and to the solutions and/or services provided hereunder. The contractor must comply with all State and Federal data and privacy laws, rules and regulations applicable to contractor under the contract.

1.1 BUSINESS REGISTRATION – Pursuant to N.J.S.A. 52:32-44, the State is prohibited from entering into a contract with an entity unless the bidder and each subcontractor named in the proposal have a valid Business Registration Certificate on file with the Division of Revenue.

The contractor and any subcontractor providing goods or performing services under the contract, and each of their affiliates, shall, during the term of the contract, collect and remit to the Director of the Division of Taxation in the Department of the Treasury the use tax due pursuant to the "Sales and Use Tax Act, P.L. 1966, c. 30 (N.J.S.A. 54:32B-1 et seq.) on all their sales of tangible personal property delivered into the State. Any questions in this regard can be directed to the Division of Revenue at (609) 292-1730. Form NJ-REG can be filed online at <http://www.state.nj.us/treasury/revenue/busregcert.shtml>.

1.2 ANTI-DISCRIMINATION - All parties to any contract with the State agree not to discriminate in employment and agree to abide by all anti-discrimination laws including those contained within N.J.S.A. 10:2-1 through N.J.S.A. 10:2-4, N.J.S.A. 10:5-1 et seq. and N.J.S.A. 10:5-31 through 10:5-38, and all rules and regulations issued thereunder are hereby incorporated by reference.

1.3 ADDITIONAL AFFIRMATIVE ACTION REQUIREMENTS -

N.J.S.A. 10:5-33 and N.J.A.C. 17:27-3.5 require that during the performance of this contract, the contractor must agree as follows:

- a) The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will take affirmative action to ensure that such applicants are recruited and employed, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause;
- b) The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex;
- c) The contractor or subcontractor where applicable, will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice, to be provided by the agency contracting officer, advising the labor union or workers' representative of the contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

N.J.A.C. 17:27-3.7 requires all contractors and subcontractors, if any, to further agree as follows;

1. The contractor or subcontractor agrees to make good faith efforts to meet targeted county employment goals established in accordance with N.J.A.C. 17:27-5.2.
2. The contractor or subcontractor agrees to inform in writing its appropriate recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, and labor unions, that it does not discriminate on the basis of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

State of New Jersey

Compliance Terms and Conditions

3. The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job-related testing, as established by the statutes and court decisions of the State of New Jersey and as established by applicable Federal law and applicable Federal court decisions.
 4. In conforming with the targeted employment goals, the contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.
- 1.4 PREVAILING WAGE ACT** - Pursuant to the New Jersey Prevailing Wage Act (N.J.S.A. 34: 11-56.26 *et seq.*), contractor guarantees that it has not been suspended or debarred by the Commissioner, New Jersey Department of Labor and Workforce Development, for violation of the provisions of the Prevailing Wage Act and/or the Public Works Contractor Registration Acts; contractor also guarantees that it will comply with the provisions of the Prevailing Wage and Public Works Contractor Registration Acts, where required and to the extent applicable to this contract.
- 1.5 AMERICANS WITH DISABILITIES ACT** - The contractor must comply with all provisions of the Americans with Disabilities Act (ADA), P.L 101-336, in accordance with 42 U.S.C. 12101, *et seq.*
- 1.6 MACBRIDE PRINCIPLES** – The contractor must certify pursuant to N.J.S.A. 52:34-12.2 that it either has no ongoing business activities in Northern Ireland and does not maintain a physical presence therein or that it will take lawful steps in good faith to conduct any business operations it has in Northern Ireland in accordance with the MacBride principles of nondiscrimination in employment as set forth in N.J.S.A. 52:18A-89.5 and in conformance with the United Kingdom's Fair Employment (Northern Ireland) Act of 1989, and permit independent monitoring of their compliance with those principles.
- 1.7 PAY TO PLAY PROHIBITIONS** – Pursuant to N.J.S.A. 19:44A-20.13 *et seq.* (L.2005, c. 51), and specifically, N.J.S.A. 19:44A-20.21, it shall be a breach of the terms of the contract for the business entity to:
- a. make or solicit a contribution in violation of the statute;
 - b. knowingly conceal or misrepresent a contribution given or received;
 - c. make or solicit contributions through intermediaries for the purpose of concealing or misrepresenting the source of the contribution;
 - d. make or solicit any contribution on the condition or with the agreement that it will be contributed to a campaign committee or any candidate or holder of the public office of Governor, or to any State or county party committee;
 - e. engage or employ a lobbyist or consultant with the intent or understanding that such lobbyist or consultant would make or solicit any contribution, which if made or solicited by the business entity itself, would subject that entity to the restrictions of the Legislation;
 - f. fund contributions made by third parties, including consultants, attorneys, family members, and employees;
 - g. engage in any exchange of contributions to circumvent the intent of the Legislation; or
 - h. directly or indirectly through or by any other person or means, do any act which would subject that entity to the restrictions of the Legislation.
- 1.8 POLITICAL CONTRIBUTION DISCLOSURE** – The contractor is advised of its responsibility to file an annual disclosure statement on political contributions with the New Jersey Election Law Enforcement Commission (ELEC), pursuant to N.J.S.A. 19:44A-20.27 (L. 2005, c. 271, §3 as amended) if in a calendar year the contractor receives one or more contracts valued at \$50,000.00 or more. It is the contractor's responsibility to determine if filing is necessary. Failure to file can result in the imposition of penalties by ELEC. Additional information about this requirement is available from ELEC by calling 1(888) 313-3532 or on the internet at <http://www.elec.state.nj.us/>.
- 1.9 STANDARDS PROHIBITING CONFLICTS OF INTEREST** - The following prohibitions on contractor activities shall apply to all contracts or purchase agreements made with the State of New Jersey, pursuant to Executive Order No. 189 (1988).
- a. No vendor shall pay, offer to pay, or agree to pay, either directly or indirectly, any fee, commission, compensation, gift, gratuity, or other thing of value of any kind to any State officer or employee or special State officer or employee, as defined by N.J.S.A. 52:13D-13b. and e., in the Department of the

State of New Jersey

Compliance Terms and Conditions

- Treasury or any other agency with which such vendor transacts or offers or proposes to transact business, or to any member of the immediate family, as defined by N.J.S.A. 52:13D-13i., of any such officer or employee, or partnership, firm or corporation with which they are employed or associated, or in which such officer or employee has an interest within the meaning of N.J.S.A. 52: 13D-13g.
- b. The solicitation of any fee, commission, compensation, gift, gratuity or other thing of value by any State officer or employee or special State officer or employee from any State vendor shall be reported in writing forthwith by the vendor to the Attorney General and the Executive Commission on Ethical Standards.
 - c. No vendor may, directly or indirectly, undertake any private business, commercial or entrepreneurial relationship with, whether or not pursuant to employment, contract or other agreement, express or implied, or sell any interest in such vendor to, any State officer or employee or special State officer or employee having any duties or responsibilities in connection with the purchase, acquisition or sale of any property or services by or to any State agency or any instrumentality thereof, or with any person, firm or entity with which he is employed or associated or in which he has an interest within the meaning of N.J.S.A. 52: 130-13g. Any relationships subject to this provision shall be reported in writing forthwith to the Executive Commission on Ethical Standards, which may grant a waiver of this restriction upon application of the State officer or employee or special State officer or employee upon a finding that the present or proposed relationship does not present the potential, actuality or appearance of a conflict of interest.
 - d. No vendor shall influence, or attempt to influence or cause to be influenced, any State officer or employee or special State officer or employee in his official capacity in any manner which might tend to impair the objectivity or independence of judgment of said officer or employee.
 - e. No vendor shall cause or influence, or attempt to cause or influence, any State officer or employee or special State officer or employee to use, or attempt to use, his official position to secure unwarranted privileges or advantages for the vendor or any other person.
 - f. The provisions cited above in paragraphs 2.8a through 2.8e shall not be construed to prohibit a State officer or employee or Special State officer or employee from receiving gifts from or contracting with vendors under the same terms and conditions as are offered or made available to members of the general public subject to any guidelines the Executive Commission on Ethical Standards may promulgate under paragraph 3c of Executive Order No. 189.

- 1.10 NOTICE TO ALL CONTRACTORS SET-OFF FOR STATE TAX NOTICE** - Pursuant to L 1995, c. 159, effective January 1, 1996, and notwithstanding any provision of the law to the contrary, whenever any taxpayer, partnership or S corporation under contract to provide goods or services or construction projects to the State of New Jersey or its agencies or instrumentalities, including the legislative and judicial branches of State government, is entitled to payment for those goods or services at the same time a taxpayer, partner or shareholder of that entity is indebted for any State tax, the Director of the Division of Taxation shall seek to set off that taxpayer's or shareholder's share of the payment due the taxpayer, partnership, or S corporation. The amount set off shall not allow for the deduction of any expenses or other deductions which might be attributable to the taxpayer, partner or shareholder subject to set-off under this act.

The Director of the Division of Taxation shall give notice to the set-off to the taxpayer and provide an opportunity for a hearing within thirty (30) days of such notice under the procedures for protests established under R.S. 54:49-18. No requests for conference, protest, or subsequent appeal to the Tax Court from any protest under this section shall stay the collection of the indebtedness. Interest that may be payable by the State, pursuant to P.L. 1987, c.184 (c.52:32-32 *et seq.*), to the taxpayer shall be stayed.

- 1.11 COMPLIANCE - STATE LAWS; JURISDICTION** - It is agreed and understood that any contracts and/or orders shall be governed and construed and the rights and obligations of the parties hereto shall be determined in accordance with the laws of the STATE OF NEW JERSEY, without giving effect to its conflict of laws. Any action brought regarding the contract or products or services purchased thereunder shall be filed in the appropriate Division of the State of New Jersey Superior Court.

- 1.12 OWNERSHIP DISCLOSURE** - In accordance with N.J.S.A. 52:25-24.2, contractor shall disclose the names and addresses of all of its owners holding 10% or more of the corporation's stock or interest during the term of the contract, by submitting an Ownership Disclosure Form at time of contract award. The contractor has the continuing obligation to notify the Division of any change in its ownership affecting 10% or more of its ownership as soon as such change has been completed.

State of New Jersey

Compliance Terms and Conditions

- 1.13 PROHIBITED INVESTMENT IN IRAN** - Pursuant to N.J.S.A. 52:32-55 et seq., the contractor must utilize the Disclosure of Investment Activities in Iran form to certify that neither the contractor, nor one of its parents, subsidiaries, and/or affiliates (as defined in N.J.S.A. 52:32-56(e)(3)), is listed on the Department of the Treasury's List of Persons or Entities Engaging in Prohibited Investment Activities in Iran and that neither the contractor, nor one of its parents, subsidiaries, and/or affiliates, is involved in any of the investment activities set forth in N.J.S.A. 52:32-56(f). If the contractor is unable to so certify, the contractor shall provide a detailed and precise description of such activities as directed on the form.
- 2. LAW REQUIRING MANDATORY COMPLIANCE BY CONTRACTORS UNDER CIRCUMSTANCES SET FORTH IN LAW OR BASED ON THE TYPE OF CONTRACT**
- 2.1 COMPLIANCE - CODES** – The contractor must comply with NJUCC and the latest NEC70, B.O.C.A. Basic Building code, OSHA and all applicable codes for this requirement. The contractor shall be responsible for securing and paying all necessary permits, where applicable.
- 2.2 PUBLIC WORKS CONTRACTOR REGISTRATION ACT** - The New Jersey Public Works Contractor Registration Act requires all contractors, subcontractors and lower tier subcontractor(s) who engage in any contract for public work as defined in N.J.S.A. 34:11-56.26 be first registered with the New Jersey Department of Labor and Workforce Development. Any questions regarding the registration process should be directed to the Division of Wage and Hour Compliance at (609) 292-9464.
- 2.3 COMPLIANCE WITH ACCESSIBILITY STANDARDS** – The contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.
- 2.4 BUILDING SERVICE** – Pursuant to N.J.S.A. 34:11-56.58 et seq., in any contract for building services, as defined in N.J.S.A. 34:11-56.59, the employees of the contractor or subcontractors shall be paid prevailing wage for building services rates, as defined in N.J.S.A. 34:11.56.59. The prevailing wage shall be adjusted annually during the term of the contract.
- 2.5 THE WORKER AND COMMUNITY RIGHT TO KNOW ACT** - The provisions of N.J.S.A. 34:5A-I et seq. which require the labeling of all containers of hazardous substances are applicable to this contract. Therefore, all goods offered for purchase to the State must be labeled by the contractor in compliance with the provisions of the statute.
- 2.6 BUY AMERICAN** – Pursuant to N.J.S.A. 52:32-1, if applicable to the contract, if manufactured items or farm products will be provided under this contract to be used in a public work, they shall be manufactured or produced in the United States and the contractor shall be required to so certify.



Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

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

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

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

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

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

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.

Data means all information, whether in oral or written (including electronic) form, 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	Crime Insurance Minimum Insurance Coverage
Low	\$2,000,000	\$2,000,000
Moderate	\$5,000,000	\$5,000,000
High	\$10,000,000	\$10,000,000

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

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

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

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

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing

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

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

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

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

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

19. Ordering

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

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

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

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

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

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

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

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

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

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

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating

Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

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

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

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. 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.

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.

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.

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

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

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

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

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

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

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

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

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

26. Records Administration and Audit.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Services it acquires from this Master Agreement.

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

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

32. Transition Assistance:

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

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

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

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

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

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

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

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

37. Governing Law and Venue

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Security Incident or Data Breach Notification:

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

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

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

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

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

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

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

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Exhibit 2 to the Master Agreement: Platform-as-a-Service

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

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

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

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

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

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

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

b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

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

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

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably

requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

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

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

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

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

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

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

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

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

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

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

Exhibit 3 to the Master Agreement: Infrastructure-as-a-Service

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

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

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

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

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

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach related to Purchasing Entity's Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

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

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

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA.

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

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

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

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

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

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

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

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

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted

and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

- a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.
- b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.
- c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

- a. The Contractor shall provide reports on a schedule specified in the SLA to the Contractor directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to in the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Contractor. The report will be sufficient to enable the Purchasing Entity to perform security analysis, resource change tracking and compliance auditing
- b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

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

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

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

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

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

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

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

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

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

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

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

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

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

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

Exhibit C – Master Agreement

Attachment 1 – Scope Addendum

STATE OF NEW JERSEY

PARTICIPATING ADDENDUM AND STANDARD TERMS AND CONDITIONS

Under

**NASPO ValuePoint Contract for Cloud Solutions
[State of Utah Master Contract Number AR2478]**

Scope Addendum

As set forth in Section 2.0, Scope of Participating Addendum, the scope of Products and Services that may be procured by Authorized Purchasers defined in Section 6.0(1) of this Participating Addendum (State Agencies) shall be those Products and Services established below. Contractor may only offer State Agencies the Products and Services from the following cloud service providers:

-) Amazon
-) Microsoft

Contractor may also provide State Agencies cloud related Services within the scope of its Master Agreement.

For all other Authorized Purchasers, the full suite of Product and Service offerings available under the Master Agreement may be procured under this Participating Addendum.