Contract # AR2482

STATE OF UTAH COOPERATIVE CONTRACT

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

Environmental Systems Research Institute, Inc.		
Name		
380 New York Street		
Address		
Redlands	CA	92373
City	State	Zip

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

Contact Person Robin Espinoza Phone 909-793-2853 x3918 Email respinoza@esri.com
Vendor #67045E 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: Contractor's Terms and Conditions

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

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

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

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

CONTRACTOR

Contractor's signature — Date: JAN 20 2017

William C. Fleming
Managing Business Attorney
Type or Print Name and Title

STATE

Director, Division of Purchasing — Date: 1. 23. 2017

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

(Revision 16 June 2016)

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

8. Confidentiality, Non-Disclosure, and Injunctive Relief

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

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

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

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

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

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

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

10. Defaults and Remedies

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

(1) Nonperformance of contractual requirements; after sufficient notification is provided by the Contractor providing an opportunity to cure. or

(2) A material breach of any term or condition of this Master Agreement; that remains uncured after 30 days written notice describing said breach 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 (collectively the Indemnified Parties) , from and against claims, damages losses, liabilities, and all causes of action including reasonable attorneys' fees arising out of any claim for bodily injury, death, or property damage (except for databases not subject to a reasonable backup program brought against any of the Indemnified Parties to the extent arising from any negligent act, or omission or willful misconduct by Contractor, its subcontractors or their respective directors, officers , employees or agents.

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 ("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 U.S. Copyright rights ("Intellectual Property Claim") of another person or entity ***provided that***

(a) The Entity promptly notifies Esri in writing of the claim thereof;

(b) Esri has sole control of the defense of any actions and negotiations related to the defense or settlement of any claim; and

(c) The Entity cooperates fully in the defense of the claim.

(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.

If Esri believes that a Deliverable is or will become the subject of an infringement claim, or in the event that use of a Deliverable is enjoined, ESRI, at its own expense, may either (i) obtain the right for Entity to continue using the Deliverable or (ii) modify the Deliverable to make it non-infringing while maintaining substantially similar software functionality or data/informational content. If neither of such alternatives is commercially practical, the infringing items shall be returned to Esri and Esri's sole liability shall be to refund development fees paid by Entity prorated on a twenty percent (20%) per year straight line depreciation basis over a five (5) year period from the date of acceptance.

Esri shall have no obligation hereunder to defend Entity or to pay any resulting costs, damages, or reasonable attorneys' fees for or with respect to any claims, actions, or demands alleging (i) infringement that arises by reason of combination of noninfringing items, however acquired, with any items not supplied by Esri; (ii) infringement to the extent arising from material alteration of the Deliverable by anyone other than ESRI, its agents, or its contractors; (iii) the direct or contributory infringement of any process patent by Licensee through the use of the Deliverable other than a process patent that is necessarily infringed by the internal processes executed within the Deliverable itself when the Deliverable is executed for its intended purpose; (iv) continued allegedly infringing activity by Esri after it has been notified of the possible infringement; (v) continued allegedly infringing activity by Entity to the extent it arises from failure of Entity to use the updated or modified Deliverable provided by Esri for avoiding infringement; or (vi) infringement that arises from Esri's compliance with specifications furnished by Esri.

THE FOREGOING STATES THE ENTIRE OBLIGATION OF ESRI WITH RESPECT TO INFRINGEMENT OR ALLEGATION OF INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS OF ANY THIRD PARTY.

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. Clarification on Professional Liability: The Professional liability limits are included in the Technical E and O policy which well exceeds the limits specified under (2) Cloud Minimum Insurance coverage.

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, cancellation, of the coverage contained in such policy shall have effect unless the named Participating Order Entity has been given at least 30 days prior written notice. Clarification: Esri's insurance company will not provide notice to entities for any material alteration or expiration. They will only issue notices to the contractor. (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

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

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

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

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

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

19. Ordering

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

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

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

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

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

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

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

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

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

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

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract)

used by the Purchasing Entity to place the Order.

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

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

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

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

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

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

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

[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.

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: With the exception of Service packages and or Managed Services upfront fees, 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. Audits conducted pursuant to this provision shall be in accordance with the established policies and procedures of the auditing agency and shall exclude Contractor's general, administrative, and profit percentages. 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: Specific ownership provisions and license grants are covered within the applicable Contractor terms and conditions (Managed Services, Service Packaged, and Professional Services.

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.

Warranty - Managed Services: Contractor warrants that there is no outstanding contract, commitment, or agreement to which Contractor is a party or legal impediment of any kind known to Contractor that conflicts with this Addendum or might limit, restrict, or impair the rights granted to Customer hereunder.
The Ordering Entity warrants and represents that it or its political subdivision and/or using entities has the full authority and right from the owner or any third party to grant permission(s) to use Customer Content offered and submitted herein to Contractor.

The Ordering Entity warrants and represents that Customer Content does not

(a) Infringe on any proprietary rights of third persons or contain any information that is deemed unlawful, libelous, violative of any person's right to privacy and/or publicity, obscene, pornographic, or indecent;

(b) Violate any law, statute, ordinance, or regulation, including, without limitation, the laws and regulations governing export control, personally identifiable information, unfair competition, antidiscrimination, or false advertising; or

(c) Contain any viruses, Trojan horses, trap doors, back doors, worms, time bombs, cancel bots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept, corrupt, or expropriate any system, data, or personal information.

DISCLAIMER OF WARRANTIES

WITH THE EXCEPTION OF THE LIMITED WARRANTY SET FORTH IN SUBSECTION 31 ABOVE, CONTRACTOR DISCLAIMS, AND THIS AGREEMENT EXPRESSLY EXCLUDES, ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION (i) THAT THE MANAGED SERVICES WILL OPERATE WITHOUT INTERRUPTION AND ARE COMPATIBLE WITH ALL EQUIPMENT AND SOFTWARE CONFIGURATIONS, OR (ii) ANY AND ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINTERFERENCE, SYSTEM INTEGRATION, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.

Data Disclaimer. IN THE EVENT THAT ANY CONTRACTOR DATA IS PROVIDED UNDER THIS ADDENDUM, THE CONTRACTOR DATA HAS BEEN OBTAINED FROM SOURCES BELIEVED TO BE RELIABLE, BUT ITS ACCURACY AND COMPLETENESS ARE NOT GUARANTEED. THE CONTRACTOR DATA MAY CONTAIN SOME NONCONFORMITIES, DEFECTS, ERRORS, OR OMISSIONS. THE CONTRACTOR DOES NOT WARRANT THAT THE CONTRACTOR DATA WILL MEET CUSTOMER'S NEEDS OR EXPECTATIONS, THAT THE USE OF THE CONTRACTOR DATA WILL BE UNINTERRUPTED, OR THAT ALL NONCONFORMITIES CAN OR WILL BE CORRECTED. CONTRACTOR IS NOT INVITING RELIANCE ON THIS CONTRACTOR DATA, AND CUSTOMER SHOULD ALWAYS VERIFY ACTUAL CONTRACTOR DATA INCLUDING, BUT NOT LIMITED TO, MAP, SPATIAL, RASTER, AND TABULAR INFORMATION.

Internet Disclaimer. CUSTOMER EXPRESSLY ACKNOWLEDGES AND AGREES THAT THE INTERNET (INCLUDING, WITHOUT LIMITATION, THE WEB) IS A NETWORK OF PRIVATE AND PUBLIC NETWORKS, AND THAT (i) THE INTERNET IS NOT A SECURE INFRASTRUCTURE, (ii) CONTRACTOR HAS NO CONTROL OVER THE INTERNET, AND (iii) CONTRACTOR IS NOT LIABLE FOR DAMAGES UNDER ANY THEORY OF LAW RELATED TO THE DISCONTINUANCE OF OPERATION OF ANY PORTION OF THE INTERNET OR POSSIBLE REGULATION OF THE INTERNET THAT MIGHT RESTRICT OR PROHIBIT THE OPERATION OF THE WEB SITE.

Contractor does not warrant that all Managed Services will be available outside the United States.

Warranty – Professional Services: Contractor warrants for a period of Ninety (90) days from the date of performance that the Services will conform to the professional and

technical standards in the software industry. During the limited warranty period, the Ordering Entity may require Contractor to re-perform the Services, at no additional cost to the Ordering Entity, if the Services do not substantially conform to the professional and technical standards of the software industry. Service Contractor warrants for a period of Ninety (90) days from the date of performance that the Services will conform to the professional and technical standards in the software industry. During the limited warranty period, the Ordering Entity may require Contractor to re-perform the Services, at no additional cost to the Ordering Entity, if the Services do not substantially conform to the professional and technical standards of the software industry. Services Output is provided "AS IS" without warranty of any kind.

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.

The Contractor request the addition of the following provisions to the contract document:

DEFINITIONS

i. "Task Order" means an order for professional services issued under this Agreement in substantially the same format as the sample task order form attached as Attachment A.
ii. "Custom Software" means all or any portion of the computer software code, components, dynamic link libraries (DLLs), and programs delivered on any media provided in source, object, or executable code format(s), inclusive of backups, updates, or merged copies permitted hereunder or subsequently supplied under any Task Order, exclusive of Commercial off-the-Shelf Software, or COTS Software.
iii. "Technical Data" means, without limitation, all technical materials including formula, compilations, software code or programs, methods, techniques, know-how, technical assistance, processes, algorithms, designs, data dictionaries and models, schematics, user documentation, training documentation, specifications, drawings, flowcharts, briefings, test or quality control procedures, or other similar information supplied or disclosed by CONTRACTOR under any Task Order. Technical Data does not include COTS Software, COTS data, or COTS documentation, which must be licensed separately by Ordering Entity under CONTRACTOR's commercial Software license.
iv. "Map Data" means any digital dataset(s) including geographic, vector data coordinates, raster, or associated tabular attributes supplied by either party for use in the performance of any Task Order.
v. "Deliverables" means Custom Software, Technical Data, or Map Data specified for delivery or use by Ordering Entity under a firm fixed price Task Order.
vi. "Commercial off-the-Shelf Software" or "COTS Software" means all or any portion of CONTRACTOR's proprietary software technology accessed or downloaded from an authorized CONTRACTOR Web site or delivered on any media in any format, including backups, updates, service packs, patches, hot fixes, or permitted merged copies, available under license to the general public.
vii. "Services" means consulting support being performed by CONTRACTOR on a time and materials hourly basis in exchange for compensation from the Ordering Entity.

viii. "Services Output" means any tangible output produced as a result of the Services provided by CONTRACTOR under this Agreement. Services Output can include, but is not limited to, reports, training materials, and Custom Software.

Contractor shall provide Deliverables and/or Services as specified in a specific Task Order relating to the COTS Software identified in the Task Order.

The parties agree that the services and deliverables provided under this Contract shall be in accordance with the following acceptance criteria:

ACCEPTANCE

A. For Time and Materials Task Orders. Services are provided strictly on a time and materials basis subject to the task order not-to-exceed funding limit. The Services delivered will be deemed accepted and in compliance with the professional and technical standards of the software industry unless Contractor is notified otherwise by the Ordering Entity within ten (10) days after delivery.

B. For Firm Fixed Price Task Orders. Deliverables for fixed price Task Orders shall be categorized as follows:

i. "DELIVERABLE ACCEPTED" means a Deliverable conforming to applicable Task Order(s) with no more than minor nonconformities. Ordering Entity shall complete its acceptance review within ten (10) working days of receiving each Deliverable.
ii. "DELIVERABLE ACCEPTED WITH REWORK" means a deliverable substantially conforming to applicable Task Order(s), but having a significant number of identified nonconformities and accepted subject to rework by Contractor. Contractor shall rework the Deliverable for the identified nonconformities and resubmit it within thirty (30) days. Ordering Entity will rerun its acceptance review for the nonconformities detected in the initial review within ten (10) working days of such resubmission and will reclassify the deliverable as either DELIVERABLE ACCEPTED or DELIVERABLE REJECTED.
iii. "DELIVERABLE REJECTED" means a Deliverable that fails to substantially conform to applicable Task Order(s). CONTRACTOR shall rework the Deliverable and resubmit it to Ordering Entity within thirty (30) days, at which time Ordering Entity shall have ten (10) working days to rerun its acceptance review and reclassify the deliverable as either DELIVERABLE ACCEPTED or DELIVERABLE REJECTED.

The Ordering Entity agrees it shall not use any Deliverable in its business operations before acceptance as described in B.i. or B.ii. If Contractor does not receive within ten (10) working days after delivery written notice that the Deliverable is "ACCEPTED WITH REWORK" or "REJECTED" in accordance with B. ii. or Bili., or if

the Ordering Entity uses the Deliverable in its business operations, the Deliverable shall be deemed, as of the first to occur of either of these events, to have been accepted.

ORDERING PROCESS/ TASK ORDERS

Unless otherwise provided by Contractor in writing, C's Contracts Manager for the Professional Services Division is authorized to agree to Task Orders. Ordering Entity shall provide advanced written notification of the name and title of the representative authorized to sign Task Orders and bind Ordering Entity. Each party may enter into Task Orders at its sole discretion and shall not have any obligation under a Task Order until it is signed by both parties.

Each party shall identify in writing the project manager who is responsible for the Services or Deliverables specified in Task Orders. By written notice, either party may replace the project manager at any time with a similarly qualified person.

The period of performance of each Task Order shall be specified in each Task Order/ Ordering Document

RESERVATION OF OWNERSHIP AND GRANT OF LICENSE

Except as specifically granted in this Section, Contractor or its licensors own and retain all right, title, and interest in the Deliverables and Services Output. This Agreement does not transfer ownership rights of any description in the Deliverables or Services Output to the Ordering Entity or any third party. Subject to the terms and conditions set forth in this Agreement and effective upon the transfer, by any means, of the Deliverables or Services Output to the Ordering Entity, CONTRACTOR hereby grants to Ordering Entity a nonexclusive, worldwide license in the Deliverables or Services Output to use, modify, and reproduce the Deliverables or Services Output in connection with Ordering Entities authorized use of COTS Software. The license grant in the immediately preceding sentence does not apply to Map Data, which the Ordering Entity must separately and directly license from the vendor.

The Ordering entity shall retain any patent, copyright, or trademark or proprietary notices on all items licensed under this Agreement and shall take other necessary steps to protect CONTRACTOR's or its licensor's intellectual property rights.

CONFIDENTIALITY OF DELIVERABLES AND SERVICES OUTPUT

Unless otherwise agreed in writing, the Deliverables and Services Output are CONTRACTOR confidential information, and Ordering Entity shall preserve and protect the confidentiality of said Deliverables and Services Output. Insofar as its rights may be legally restricted, Ordering Entity agrees not to reverse engineer or decompile

Deliverables or Services Output delivered only in object code, executable code, or formats subject to similar or greater means of access control (collectively, "Secure Formats"). For Deliverables or Services Output delivered in source code or other human-readable formats, Ordering Entity shall have met its obligations under this Article if its disclosure of Deliverables or Services Output is limited to Deliverables or Services Output in Secure Formats, *provided that* the means for reverse engineering, decompiling, or disassembling such Deliverables or Services Output is withheld from such disclosure, and the person or entity in receipt of such Deliverables or Services Output similarly agrees not to perform such acts or allow others to do so.

Except as provided in the preceding paragraph, Ordering Entity shall not disclose any Deliverables or Services Output to employees or third parties which have been specifically marked as “Confidential” without the advanced written consent of CONTRACTOR. However, Ordering Entity may, without such consent, make such disclosures to employees as are reasonably required for the Ordering Entity's authorized use of the COTS Software, provided that such disclosure is strictly limited to the portions of the Deliverables or Services Output needed for that purpose. The disclosures permitted under this paragraph shall not relieve Ordering Entity of its obligation to maintain the Deliverables or Services Output in confidence and comply with all applicable laws and regulations of the United States.

Ordering Entity shall not have any obligation to protect any part of a Deliverable or Services Output that it can prove: (i) was in Ordering Entity's possession before receipt from CONTRACTOR; (ii) is or becomes a matter of public knowledge through no fault of Ordering Entity; (iii) is rightfully disclosed by a third party without a duty of confidentiality; (iv) is disclosed by CONTRACTOR to a third party without a duty of confidentiality; (v) is independently developed by Ordering Entity; or (vi) is required to be disclosed by operation of law.

CHANGES TO SCOPE OF WORK

Ordering Entity may, at any time, request changes within the general scope of an open Task Order. If the parties agree to such changes and such changes cause an increase or decrease in the cost or time required to provide a Deliverable under any Task Order (regardless of whether the Deliverable itself is changed), an equitable adjustment in the price or schedule, or both, shall be made, and this Agreement shall be modified accordingly in writing and signed by both parties.

COMPENSATION; INVOICES

A. **For Time and Materials Task Orders.** CONTRACTOR shall prepare and submit to Ordering Entity written monthly invoices showing the compensation due for work

performed, including travel time, under Task Orders to the Ordering Entity address listed on the Task Order. The amount invoiced will be equal to the number of hours expended during the previous month multiplied by the rates for labor categories set forth in Attachment B, plus other burdened direct costs (ODCs), such as travel-related expenses. Meals and incidental expenses will be invoiced on a "per diem" basis in accordance with the limits in the most current Federal Travel Regulations.

CONTRACTOR may reallocate the budget between activities, labor categories, and ODCs as necessary to facilitate the work effort, provided the overall price is not exceeded. In the event CONTRACTOR reaches the funded not-to-exceed Task Order value and the activities are not completed, Ordering Entity may increase the order funding to allow additional work to be performed, or CONTRACTOR may stop work without further obligation or liability.

B. For Firm Fixed Price Task Orders. Unless otherwise specified in a Task Order, CONTRACTOR shall prepare and submit monthly invoices based on the percent complete for each Deliverable as of the end of the preceding month. Upon acceptance of all Deliverables under a Task Order, the unpaid balance of the total Task Order value is due.

C. Payment. Ordering Entity shall pay each invoice no later than thirty (30) days after receipt thereof. Payment shall be made to the CONTRACTOR address identified on original CONTRACTOR invoices.

LIMITATION OF LIABILITY

A. Disclaimer of Certain Types of Liability. IN NO EVENT SHALL CONTRACTOR OR ITS LICENSOR(S) BE LIABLE TO ORDERING ENTITY FOR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOST PROFITS; LOST SALES OR BUSINESS EXPENDITURES; INVESTMENTS; OR COMMITMENTS IN CONNECTION WITH ANY BUSINESS, LOSS OF ANY GOODWILL, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT OR USE OF THE DELIVERABLES OR SERVICES OUTPUT, HOWEVER CAUSED, ON ANY THEORY OF LIABILITY, AND WHETHER OR NOT CONTRACTOR OR ITS LICENSOR(S) HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY.

B. General Limitation of Liability. IN NO EVENT WILL CONTRACTOR'S TOTAL CUMULATIVE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT OR USE OF THE DELIVERABLES OR SERVICES OUTPUT, FROM ALL CAUSES OF ACTION OF ANY KIND, INCLUDING, BUT NOT LIMITED TO, CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF WARRANTY, MISREPRESENTATION, OR OTHERWISE, EXCEED TWO TIMES THE AMOUNTS PAID TO CONTRACTOR BY ORDERING ENTITY FOR THE DELIVERABLES OR SERVICES OUTPUT FROM WHICH THE LIABILITY DIRECTLY AROSE or $1,000,000, whichever is greater.

C. Applicability of Disclaimers and Limitations. Ordering Entity agrees that the limitations of liability and disclaimers set forth in this Agreement will apply regardless of whether Ordering Entity has accepted the Deliverables, or any other product or service delivered by CONTRACTOR. The parties agree that CONTRACTOR has set its prices and entered into this Agreement in reliance upon the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose or cause consequential loss), and that the same form an essential basis of the bargain between the parties.

RESTRICTIONS ON SOLICITATION

Ordering Entity shall not solicit for hire any CONTRACTOR employee who is associated with efforts called for under this Agreement during the term of this Agreement and for a period of one (1) year thereafter. The foregoing shall in no way restrict Ordering Entity from publicly advertising positions for hire in newspapers, professional magazines, or Internet postings.

TAXES

Values specified in Task Orders are exclusive of Ordering Entity, local, and other taxes or charges (including, without limitation, custom duties, tariffs, and value-added taxes, but excluding income taxes payable by CONTRACTOR) To the extent the Participating entity is taxable, in the event any unforeseen taxes or charges become applicable to Deliverables or Services Output, Ordering Entity shall pay any such taxes upon receipt of written notice from Contractor, that they are due.

NOTICE

All notice required by this Agreement shall be in writing to the parties at the following respective addresses, or to such other address as a party may subsequently specify in a notice provided in the manner described in this Article, and shall be deemed to have been received (i) upon delivery in person; (ii) upon the passage of three (3) days following post by first class registered or certified mail, return receipt requested, with

postage prepaid; (iii) upon the passage of two (2) days following post by overnight receipted courier service; or (iv) upon transmittal by confirmed e-mail or facsimile, provided that if sent by e-mail or facsimile, a copy of such notice shall be concurrently sent by U.S. certified mail, return receipt requested and postage prepaid, with an indication that the original was sent by e-mail or facsimile and the date of its transmittal:

Ordering Entity:

_____

_____

Attn.: _____

Tel.: _____

Fax: _____

Contractor: Environmental Systems Research Institute, Inc.
380 New York Street
Redlands, CA 92373-8100
USA
Project/Technical Notice—Attn.: Robin Espinoza,
Senior Contract Administrator
Tel.: 909-793-2853, extension 3918
Fax: 909-307-3034
Legal Notice—Attn.: Contract Manager
Tel.: 909-793-2853, extension 1590
Fax: 909-307-3020
With a copy to Robin Espinoza, Senior, Contract Administrator

Notice for non-U.S. Ordering Entities shall be deemed to have been received (i) upon delivery in person; (ii) upon the passage of seven (7) days following post by international courier service with shipment tracking provisions; or (iii) upon transmittal by confirmed e-mail or facsimile, provided that if sent by e-mail or facsimile, a copy of such notice shall be concurrently sent by receipted international courier service, with an indication that the original was sent by e-mail or facsimile and the date of its transmittal.

ASSIGNMENT AND DELEGATION

CONTRACTOR may, in whole or in part, assign any of its rights or delegate any performance under this Agreement, provided that CONTRACTOR shall remain responsible for the performance it delegates. This Agreement binds and benefits successors or assigns permitted under this Article 18.

IMPLIED WAIVER

The failure of either party to enforce any provision of this Agreement shall not be deemed a waiver of the provisions or of the right of such party thereafter to enforce that or any other provision.

EQUITABLE RELIEF

Ordering Entity agrees that any breach of this Agreement by Ordering Entity will cause irreparable damage and that, in the event of such breach, in addition to any and all remedies at law, CONTRACTOR shall have the right to an injunction, specific performance, or other equitable relief in any court of competent jurisdiction to prevent violation of these terms and without the requirement of posting a bond or undertaking or proving injury as a condition for relief.

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. Contractor can comply with this requirement for EMCS, FedRAMP and AGOL.

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. All personal data would be managed under EMCS FedRAMP SaaS Offering, and AGOL is excluded as it does not encrypt data at rest. Note: Esri will not be holding any PII or PHI data in the Cloud GIS Offerings provided under this 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. Non-public data would be managed by FedRAMP or EMCS, since AGOL does not encrypt data at rest.

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. Note: Contractor can comply with EMCS, FedRAMP and AGOL.

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. Contractor can meet this for EMCS, FedRAMP and AGOL.

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 within 72 hours based on the standards set by DFARS 252.204.7012.

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. Contractor will not be holding PII or PHI in the cloud offerings under this agreement.

a. The Contractor, unless stipulated otherwise, shall notify the appropriate Purchasing Entity identified contact by telephone within 72 hours in accordance with DFARS 252.204.7012 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 72 hours in accordance with DFARS 252.204.7012 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 reasonable 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 . The cost of compliance shall in no event, exceed the limitation of liability specified in the Master contract as agreed between the Parties. (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall use reasonable efforts to 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 use reasonable efforts to notify the Purchasing Entity of receipt of a valid request by the federal entity regarding records requests associated with this contract.

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. Contractor can meet this requirement for AGOL, EMCS, FedRAMP.

b. During any period of service suspension, during the term of the Master Agreement, 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. If specified in a Participating addendum, all costs associated with compliance shall be borne by the respective Ordering entity.

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. Audits conducted pursuant to this provision shall be in

accordance with the auditing agencies policies and procedures and shall exclude Contractor's general, administrative, and profit percentages.

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. Contractor uses infrastructure from Amazon Web Services and Microsoft Azure. Our cloud infrastructure providers conduct these audits and make them available to customers at the following. https://aws.amazon.com/compliance/ and

Microsoft Azure (https//azure.microsoft.com/en-us/support/trust-center/compliance/ Note: This clarification is also applicable to the respective sessions in Exhibits 2, (PAAS) and Exhibit 3 (IAAS).

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, and upon execution of an appropriate NDA by the Purchasing Entity, the Contractor shall disclose, at its discretion, 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 will perform an annual Disaster Recovery test and will develop a plan to mitigate issues detected during the test If requested, Contractor will share the results of the test with the Purchasing Entity upon execution of an NDA.

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. Contractor will not be holding any PII or PHI data in the Cloud GIS offerings provided under this Agreement.

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. Contractor can comply with this requirement for EMCS, FedRAMP, and AGOL.

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. Any personal data would be managed under EMCS, FedRAMP, SAAS Offering, and AGOL SAAS is excluded as it does not encrypt data at rest. Note: Esri will not be holding PII or PHI data in the cloud GIS Offerings provided under this 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. Non-public data would be managed by FedRAMP, or EMCS, since AGOL does not encrypt data at rest.

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. Contractor can meet this for EMCS, FedRAMP, and AGOL.

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 report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity within 72 hours based on the standards set by DFARS 252.204.7012.

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. Contractor will not be holding PII or PHI in the Cloud offerings under this agreement.

a. The Contractor, unless stipulated otherwise, shall use reasonable efforts to notify the appropriate Purchasing Entity identified contact by telephone within 72 hours in accordance with DFARS 252.204.7012 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 72 hours by telephone in accordance with DFARS 252.204.7012 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 reasonable 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 . The cost of compliance shall in no event exceed the limitation of liability specified in the Master contract as agreed between the Parties. (5) complete all corrective actions as reasonably determined by Contractor based on root cause. This section should not be applicable as Contractor will not be holding PII or PHI in the Cloud GIS offerings provided under this Agreement.

6. Notification of Legal Requests: The Contractor shall use reasonable efforts to 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 use reasonable efforts to notify the Purchasing Entity of a receipt of a valid request by a federal entity regarding records requests associated with this contract.

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. Contractor can meet this requirement for AGOL, EMCS, FedRAMP.

b. During any period of service suspension, during the term of the Master Agreement, 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. If specified in a Participating Addendum, all costs associated with compliance shall be borne by the respective Ordering entity.

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 a Participating Addendum.

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. Audits conducted pursuant to this provision shall be in accordance with the auditing agencies policies and procedures and shall exclude Contractor's general, administrative, and profit expenses.

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. Contractor uses infrastructure from Amazon Web Services and Microsoft Azure. Our cloud infrastructure providers conduct these audits and make them available to customers at the following: https://aws.amazon.com/compliance/ and

Microsoft Azure https://azure.microsoft.com/en-us/support/trust/center/compliance

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, and upon execution of an appropriate NDA by the Purchasing Entity, the Contractor shall disclose at its discretion, 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 will work with the Purchasing Entity to perform an annual Disaster Recovery test and will develop a plan to mitigate any issues detected during the test. If requested, Contractor will share the results of the test with the Purchasing Entity upon execution of an NDA.

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. Contractor will not be holding any PII or PHI data in the Cloud GIS offerings provided under this Agreement.

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. Esri can comply with this requirement for EMCS, FedRAMP and AGOL.

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. Clarification: Any personal data would be managed under EMCS FedRAMP SAAS Offering and AGOL SAAS is excluded as it does not encrypt data at rest. Note: Esri will not be holding PII or PHI data in the cloud GIS offerings provided under this 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. Clarification: Nonpublic data would be managed by FedRAMP or EMCS, since AGOL does not encrypt data at rest.

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. Note: Esri can comply with EMCS, FedRAMP and AGOL.

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 within 72 hours based on the standards set by DFARS 252.204.7012.

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. Note: Esri will not be holding any PII or PHI data in the Cloud GIS Offerings to be provided under this agreement.

a. The Contractor, unless stipulated otherwise, shall notify the appropriate Purchasing Entity identified contact by telephone within 72 hours in accordance with DFARS252.204.7012 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 72 hours, by telephone, in accordance with DFARS 252.204.7012 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 The cost of compliance shall in no event exceed the limitation of liability specified in the Master Contract as agreed between the Parties. and (5) complete all corrective actions as reasonably determined by Contractor based on root cause. Clarification. This section should not be applicable as Esri will not be holding PII or PHI in the Cloud GIS Offerings provided under this Agreement.

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 use reasonable efforts to notify the Purchasing Entity of receipt of a valid request by a federal entity regarding records reuest associated with this contract.

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. Note: Esri can meet this requirement for AGOL EMCS FedRAMP.

b. During any period of service suspension, during the term of the Master Agreement, 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 .If specified in a Participating Addendum, all costs associated with compliance shall be borne by the respective Ordering Entity.

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. Audits conducted pursuant to this provision shall be in accordance with the auditing agencies policies and procedures and shall exclude Contractor's general, administrative and profit expenses.

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. Clarification: Esri uses infrastructure from Amazon Web Services and Microsoft Azure. Our cloud infrastructure providers conduct these audits and make them available to customers at the following; https://aws.amazon.com/compliance/

Microsoft Azure https://azure.microsoft.com/en-us/support/trust-center/compliance

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, and upon execution of an appropriate NDA by the Purchasing Entity the Contractor shall disclose, at its discretion, 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 will perform an annual Disaster Recovery test and will develop a plan to mitigate issues detected during the test. If requested, Contractor will share the results of the test with Purchasing Entities upon execution of an NDA.

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

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
GIS SaaS – ArcGIS Online	X			Public Cloud
GIS SaaS – Managed Service Bundles		X		Public Cloud Community Cloud Hybrid Cloud
GIS IaaS – Self-Service Cloud Environments Self-Service Cloud Environments can use physical Infrastructure provided by Amazon Web Services (AWS) which aligns with FedRAMP Moderate Sensitivity and ISO 27001. It will be the Purchasing Entity's responsibility to implement a solution capable of securing and storing moderate risk data		X		Public Cloud
GIS PaaS – Managed Services Bundles		X		Public Cloud Community Cloud Hybrid Cloud

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 – 0%**
Infrastructure as a Service	**Discount – 0%**
Platform as a Services	**Discount – 2%**
Value Added Services	**Discount – 2%**

Hourly Rates

Labor Categories	2017 - Offsite	2017 - Onsite
Technical Analyst	$222	$272
Technical Consultant I	$255	$305
Technical Consultant II	$278	$328
Technical Consultant III	$345	$395
Deployment Technician	$186	$236
Support Specialist	$142	$192

* Hourly labor rates have been provided for each labor category for calendar year 2017. The hourly labor rates for services that are performed after 2017 may be escalated in an amount not to exceed five percent (5%) each year.

Infrastructure as a Service (IaaS)

I. Product Offers

A. Self-Service Cloud Environments

For Purchasing Entities interested in deploying GIS in the cloud on their own, Esri offers Self-Service Cloud Environments. By subscribing to a Self-Service Cloud Environment, Purchasing Entities have the ability to self-provision infrastructure resources on-demand. Self-Service Cloud Environments serve as the gateway for cloud-enabled GIS, giving Purchasing Entities access to administration tools which allow for self-provisioning of cloud application(s), servers to support GIS and database needs, as well as storage capacity. Purchasing Entity resources will have the ability to select from a variety of cloud infrastructure providers and can select their operating systems, database management systems, and Esri ArcGIS technologies of choice. Purchasing Entity's representatives are responsible for provisioning new servers, storage, databases, and any other infrastructure required as well as deploying and managing software. The representatives may choose to set up remote access to provisioned servers and are therefore free to deploy and modify databases on demand. Upon task order award, Esri will engage with the infrastructure partner ("Infrastructure Host") selected by the Purchasing Entity to activate a dedicated cloud self-service account for the Purchasing Entity. If the Infrastructure host is Amazon Web Services, the Purchasing entity must choose an Amazon Web Service support tier at time of purchase. Esri will also train one identified individual within a Purchasing Entity for up to four hours on the cloud administration tools.

Once an Environment is provisioned, the Purchasing Entity has the ability to load data, publish web services, deploy web applications and take advantage of other cloud administration tools, such as elastic load balancing and auto-scaling. It is the Purchasing Entity's responsibility to provision, administer and manage the Environment in accordance with their desired security and operational standards. There is no Service Level Agreement associated with data, services, or applications hosted with Self-Service Cloud Environments. Organizations can use existing ArcGIS for Server licenses or choose from convenient, renewable, 1-, 3-, and 12-month term licensing. Additional terms apply to use Esri Software.

For Amazon Web Services – Current pricing can be found at http://aws.amazon.com/. If ordering services through Amazon Web Services, the Purchasing Entity must choose an Amazon Web Services support tier at time of purchase (excludes Mechanical Turk, Amazon Dev Pay and Flexible Payment Services).

For IBM SoftLayer – Current pricing can be found at http://www.softlayer.com/. If ordering services through IBM SoftLayer the Purchasing Entity receives unlimited access to IBM's technical support resources at no additional charge.

For Microsoft Azure – Current pricing can be found at https://azure.microsoft.com/en-us/. If ordering services through Microsoft Azure, the Purchasing Entity much chose an Azure Support for Customers plan at time of purchase. Esri reserves the right to change pricing for Self-provision cloud services at any time to the extent required to offset pricing changes from the Infrastructure host.

IAAS provided under AWS, IBMSoftLayer and Microsoft Azure is provided exclusively under the terms of use set forth by the Infrastructure host. Purchasing Entities access to and continued use of the IAAS Services above is conditioned upon compliance with all laws, rules, and regulations (b) compliance and agreement with the policies and procedures under which the IAAS is made available by the Infrastructure host in general and 3) conformance with Esri training provided for the use of the cloud administration tools. Esri reserves the right to update these terms and conditions at any time as promulgated by the Infrastructure Host. The Purchasing Entity agrees to comply with all Infrastructure Host terms and conditions of use.

ESRI DOES NOT WARRANT OR ASSUME ANY LIABILITY FOR THE PERFORMANCE OR OPERATION OF THE IAAS INFRASTRUCTURE HOST AND IS NOT RESPONSIBLE FOR ANY CLAIMS ARISING OUT OF THE USE OF THE SELF SERVICE CLOUD HOSTING.

ArcGIS for Server Enterprise Standard Term Licenses	Price
ArcGIS for Server Enterprise Standard (up to four cores) 30-Day Term License	$2,300
ArcGIS for Server Enterprise Standard (up to four cores) 60-Day Term License	$6,000
ArcGIS for Server Enterprise Standard (up to four cores) 365-Day Term License	$12,000

II. Value Added Services

A. Advice Services

1. System Architecture and Design – $33,100 [4-days]

Designed for Purchasing Entities building new or migrating existing GIS to the cloud, the System Architecture and Design offer will equip Purchasing Entities with the information required to plan a cloud environment to support their needs. Whether considering a range of market leading cloud infrastructure providers (Amazon AWS, Microsoft Azure, IBM SoftLayer) or debating a hybrid strategy

of on premises and cloud, an Esri consultant will lead on-site activities to assess requirements, lead discussions, and evaluate cloud design alternatives. The purpose of the engagement is to determine an appropriate cloud GIS architecture for the business drivers and technical requirements identified during this activity. As a result of these activities Purchasing Entities will receive cloud configuration recommendations in a Cloud System Architecture and Design document.

3-day – $29,900 5- day – $42,800

2. Cloud Readiness and Roadmap – $15,000

Note: *This offer is only available in conjunction with the purchase of a System Architecture and Design.*

A Purchasing Entity may choose to add a Cloud Readiness and Roadmap package to their System Architecture and Design Exercise. Leveraging the System Architecture and Design recommendations, Esri will provide consulting services to develop a Cloud Readiness Assessment and Migration Roadmap. The Cloud Readiness Assessment will classify the Purchasing Entity's GIS existing environment, workflows, services, data, and applications against cloud migration criteria and considerations. The Migration Roadmap will outline recommended migration approach, milestones, deliverables and a schedule.

3. Cloud Capacity Planning – $2,500

This service provides cloud environment and capacity recommendations for Esri products. These recommendations are based on Esri best practices and the Purchasing Entity's profile and requirements. A three-page summary of recommendations is provided.

B. Enablement Services

1. ArcGIS for Server Jumpstart for Amazon Web Services – $10,900 [3-day]

With ArcGIS for Server on Amazon Web Services (AWS), you harness the power of the cloud while maintaining full control over your environment. The ArcGIS for Server Jumpstart for Amazon Web Services enables organizations to get started with ArcGIS for Server. This service provides configuration support, technology transfer on standard topics and best practices to provide a smooth transition to AWS.

4-day – $13,300

2. ArcGIS for Server Jumpstart for Microsoft Azure– $10,900 [3-day]

With ArcGIS for Server on Microsoft Azure, you harness the power of the cloud while maintaining full control over your environment. The ArcGIS for Server Jumpstart for Microsoft Azure enables organizations to get started with ArcGIS

for Server. This service provides configuration support, technology transfer on standard topics and best practices to provide a smooth transition to Azure.

4-day – $13,300

3. ArcGIS for Server Jumpstart for IBM SoftLayer – $10,900 [3-day]

With ArcGIS for Server on IBM SoftLayer, you harness the power of the cloud while maintaining full control over your environment. The ArcGIS for Server Jumpstart for IBM SoftLayer enables organizations to get started with ArcGIS for Server. This service provides configuration support, technology transfer on standard topics and best practices to provide a smooth transition to SoftLayer.

4-day – $13,300

4. WebGIS Jumpstart – $10,900 [3-day]

The WebGIS Jumpstart gives a Purchasing Entity an introduction to the capabilities of WebGIS and demonstrates how to leverage it as part of the ArcGIS platform. Organizations will learn how to configure their cloud environment using ArcGIS Online or Portal for ArcGIS and how the cloud plays a central role in this emerging pattern.

4-day – $13,300

5. Performance and Scalability Testing – $24,900

With a Performance and Scalability package, Purchasing Entities will be able to know if their cloud environment will scale as planned with confidence. During this engagement, Esri will implement a test plan, validate the planned cloud environment, run a standard battery of testing scripts, and test execution to measure how workflows perform and how your cloud environment scales under load. Results of these tests will be summarized in a document at the completion of testing.

C. Migration Services

1. Map, data, or application migration services – $24,900

A Purchasing Entity can get support from an Esri consultant to migrate a physical or virtual GIS environment to a cloud-based environment. Cloud migration typically involves the migration of data, services, and application(s) and the Esri consultant can help with any of these activities. During the engagement, the Esri consultant will employ an “I do, we do, you do” approach, initially doing, then working side-by-side with Purchasing Entity resources, and concluding by ensuring that the Purchasing Entity’s resources are able to perform on their own.

D. Use

1. Cloud-based GIS Health Check – $13,700

This proactive activity is designed to provide early detection of potential issues by reviewing a Purchasing Entity's cloud environment. After walking through a standard set of evaluation tools with an Esri consultant, organizations will understand how their GIS systems compare to Esri best practices, where improvements can be made, and receive recommendations based on the findings.

2. Cloud GIS Performance Assessment – $24,900

Unsure what is causing slow performance in your cloud environment? Are your cloud costs growing faster than expected? This service will investigate cloud GIS system performance, including bottleneck detection and service bloat. During this engagement, an Esri expert will collect performance metrics, identify problems with system configuration and architecture, and discuss components that impact performance. Tools and methodologies will be used to isolate and diagnose performance issues. A report with findings and recommendations is provided following the on-site visit.

3. Performance Tuning - $13,700

Note: *This offer is only available in conjunction with the purchase of a Cloud Performance Assessment.*

Is a specific GIS operation experiencing slow performance? This service will focus on addressing the performance pain points already identified in the Cloud GIS Performance Assessment. Esri resources will examine operation workload, application configuration, and the operating environment. Tools and methodologies will be utilized to trace and measure the effects of parameter changes and optimization.

Platform as a Service (PaaS)

I. Product Offers

A. Managed Cloud Services Bundles

Purchasing Entities have the ability to procure the ArcGIS platform through the Esri Managed Cloud Services team. The Managed Cloud Services Bundles are designed to grant Purchasing Entities access to all of the features of ArcGIS for Server including Portal while removing the responsibilities normally associated with administering the Platform. By purchasing a Managed Cloud Service bundle, Purchasing Entities gain access to Esri's cloud *and* GIS expertise. This partnership allows a Purchasing Entity's resources the freedom to focus on delivering location value with the confidence that Esri will deliver a system to support its strategic and operational goals.

Name	Description	Monthly costs
Small	This bundle is targeted at small municipalities, individual developers, or single departments looking to deploy web applications. Purchasing entities buying the small bundle will have access to administer their ArcGIS for Server and 1 virtual desktop	$1,300
Medium	Based on our most common deployment, the Medium is ideal for counties and small states hosting GIS practice in the cloud. Includes desktops for three users and is WebGIS ready	$2,900
Large	This configuration is ideal for states hosting all GIS services in the cloud, organizations looking for multi-environment support (Dev, Test, and Production), or large web applications with thousands of users	$9,200
X-Large (FedRAMP Moderate)	Esri's X-Large Managed Service bundle is suited to large organizations looking for the security and controls guaranteed by FedRamp Moderate environments. There are 10 virtual desktops included with this bundle.	$17,600
Custom	If the bundles above do not meet a Purchasing Entity's requirements, Esri can configure and host an environment to suit its size, performance, and security needs	TBD

II. Value Added Services

A. Advice Services

1. System Architecture and Design – $33,100 [4-days]

Designed for Purchasing Entities building new or migrating existing GIS to the cloud, the System Architecture and Design offer will equip Purchasing Entities with the information required to plan a cloud environment to support their needs. Whether considering a range of market leading cloud infrastructure providers (Amazon AWS, Microsoft Azure, IBM SoftLayer) or debating a hybrid strategy of on premises and cloud, an Esri consultant will lead on-site activities to assess requirements, lead discussions, and evaluate cloud design alternatives. The purpose of the engagement is to determine an appropriate cloud GIS architecture for the business drivers and technical requirements identified during this activity. As a result of these activities Purchasing Entities will receive cloud configuration recommendations in a Cloud System Architecture and Design document.

3-day – $29,900 5- day – $42,800

2. Cloud Readiness and Roadmap – $15,000

Note: *This offer is only available in conjunction with the purchase of a System Architecture and Design.*

A Purchasing Entity may choose to add a Cloud Readiness and Roadmap package to their System Architecture and Design Exercise. Leveraging the System Architecture and Design recommendations, Esri will provide consulting services to develop a Cloud Readiness Assessment and Migration Roadmap. The Cloud Readiness Assessment will classify the Purchasing Entity's GIS existing environment, workflows, services, data, and applications against cloud migration criteria and considerations. The Migration Roadmap will outline recommended migration approach, milestones, deliverables and a schedule.

B. Enablement Services

1. ArcGIS for Server Jumpstart for the Cloud – $10,900 [3-day]

With ArcGIS for Server deployed in the cloud, you not only have access to the power of the cloud but also have full control over your environment. The ArcGIS for Server Jumpstart for the Cloud enables organizations to get started with ArcGIS for Server. This service provides configuration support, technology transfer on standard topics and best practices to provide a smooth transition to the cloud.

4-day - $13,300

2. WebGIS Jumpstart – $10,900 [3-day]

The WebGIS Jumpstart gives a Purchasing Entity an introduction to the capabilities of WebGIS and demonstrates how to leverage it as part of the ArcGIS platform. This service is ideal for organizations looking to embrace the WebGIS pattern. This is accomplished with assistance from an Esri consultant who will help Purchasing Entity resources configure their WebGIS using an ArcGIS Online or Portal for ArcGIS. They may also review how to populate a Purchasing Entity's account with organizational content, and help resources learn best practices on how to use, publish, and administer content and services with WebGIS.

4-day – $13,300

3. Proof of Concept – $32,300

Purchasing Entities looking to migrate to the cloud may not always feel confident in how a cloud-based environment will work for their organization. The Proof of Concept is designed to equip organizations with the experiences and information they need to confidently make a cloud migration decision and plan. Esri consultants will work with the Purchasing Entity resources to establish baselines for key performance metrics. The Proof of Concept will take place over three phases: Discovery, Experience, and Reporting. During the Discovery phase, an Esri consultant will work to establish will explain key cloud KPIs and establish baseline measurements for the Purchasing Entity. While in the Experience phase,

the Purchasing Entity will have access to an ArcGIS system which Esri will set-up, configure, and deploy in the cloud. Throughout the Proof of Concept, Esri will help the Purchasing Entity continue to measure the key performance metrics. At the end, the Purchasing will receive a report of how the system performed against the KPIs and how those compared to the baseline measurements.

90-day engagement. Term licensing may be added. Quotes for custom Proofs of Concept can be provided upon request.

C. Migration Services

1. Map, data, or application migration services – $24,900

A Purchasing Entity can get support from an Esri consultant to migrate a physical or virtual GIS environment to a cloud-based environment. Cloud migration typically involves the migration of data, services, and application(s) and the Esri consultant can help with any of these activities. During the engagement, the Esri consultant will employ an "I do, we do, you do" approach, initially doing, then working side-by-side with Purchasing Entity resources, and concluding by ensuring that the Purchasing Entity's resources are able to perform on their own.

D. Use

1. Cloud-based GIS Health Check – $13,700

This proactive activity is designed to provide early detection of potential issues by reviewing a Purchasing Entity's cloud environment. After walking through a standard set of evaluation tools with an Esri consultant, organizations will understand how their GIS systems compare to Esri best practices, where improvements can be made, and receive recommendations based on the findings.

2. Cloud GIS Performance Assessment – $24,900

Unsure what is causing slow performance in your cloud environment? Are your cloud costs growing faster than expected? This service will investigate cloud GIS system performance, including bottleneck detection and service bloat. During this engagement, an Esri expert will collect performance metrics, identify problems with system configuration and architecture, and discuss components that impact performance. Tools and methodologies will be used to isolate and diagnose performance issues. A report with findings and recommendations is provided following the on-site visit.

3. Performance Tuning - $13,700

Note: *This offer is only available in conjunction with the purchase of a Cloud Performance Assessment.*

Is a specific GIS operation experiencing slow performance? This service will focus on addressing the performance pain points already identified in the Cloud GIS Performance Assessment. Esri resources will examine operation workload,

application configuration, and the operating environment. Tools and methodologies will be utilized to trace and measure the effects of parameter changes and optimization.

Software as a Service

I. Product Offers

A. ArcGIS Online

Esri's secure, multitenant cloud that's scalable and ready to use. No additional hardware or software has to be purchased or installed. ArcGIS Online gives users in a Purchasing Entity's organization access to tools, basemaps, and other content to make and share maps and applications. Users can catalog and discover maps and applications; set up groups to collaborate; and share items with each other, the entire organization, or publicly. For example, without any programming, any user that's part of an ArcGIS Online organizational account can quickly share maps by embedding them in a website or blog, through social media, or by using preconfigured web application templates.

Current pricing is available at http://www.esri.com/software/arcgis/arcgisonline/purchase.

Separate terms govern this offering and can be found at:
http://www.esri.com/~/media/Files/Pdfs/legal/pdfs/mla_e204_e300/english

II. Value Add Services

A. Advice Services

1. System Architecture and Design – $33,100 [4-days]

Designed for Purchasing Entities building new or migrating existing GIS to the cloud, the System Architecture and Design offer will equip Purchasing Entities with the information required to plan a cloud environment to support their needs. Whether considering a range of market leading cloud infrastructure providers (Amazon AWS, Microsoft Azure, IBM SoftLayer) or debating a hybrid strategy of on premises and cloud, an Esri consultant will lead on-site activities to assess requirements, lead discussions, and evaluate cloud design alternatives. The purpose of the engagement is to determine an appropriate cloud GIS architecture for the business drivers and technical requirements identified during this activity. As a result of these activities Purchasing Entities will receive cloud configuration recommendations in a Cloud System Architecture and Design document.

3-day – $29,900 5- day – $42,800

2. Cloud Readiness and Roadmap – $15,000

Note: *This offer is only available in conjunction with the purchase of a System Architecture and Design.*

A Purchasing Entity may choose to add a Cloud Readiness and Roadmap package to their System Architecture and Design Exercise. Leveraging the System Architecture and Design recommendations, Esri will provide consulting services

to develop a Cloud Readiness Assessment and Migration Roadmap. The Cloud Readiness Assessment will classify the Purchasing Entity's GIS existing environment, workflows, services, data, and applications against cloud migration criteria and considerations. The Migration Roadmap will outline recommended migration approach, milestones, deliverables and a schedule.

B. Enablement Services

1. WebGIS Jumpstart – $10,900 [3-day]

The WebGIS Jumpstart gives a Purchasing Entity an introduction to the capabilities of WebGIS and demonstrates how to leverage it as part of the ArcGIS platform. This service is ideal for organizations looking to embrace the WebGIS pattern. This is accomplished with assistance from an Esri consultant who will help Purchasing Entity resources configure their WebGIS using an ArcGIS Online or Portal for ArcGIS. They may also review how to populate a Purchasing Entity's account with organizational content, and help resources learn best practices on how to use, publish, and administer content and services with WebGIS.

4-day – $13,300

C. Migration Services

1. Map, data, or application migration services – $24,900

A Purchasing Entity can get support from an Esri consultant to migrate a physical or virtual GIS environment to a cloud-based environment. Cloud migration typically involves the migration of data, services, and application(s) and the Esri consultant can help with any of these activities. During the engagement, the Esri consultant will employ an "I do, we do, you do" approach, initially doing, then working side-by-side with Purchasing Entity resources, and concluding by ensuring that the Purchasing Entity's resources are able to perform on their own.

D. Use

1. Cloud-based GIS Health Check – $13,700

This proactive activity is designed to provide early detection of potential issues by reviewing a Purchasing Entity's cloud environment. After walking through a standard set of evaluation tools with an Esri consultant, organizations will understand how their GIS systems compare to Esri best practices, where improvements can be made, and receive recommendations based on the findings.

Notice of Proprietary Information:

The information in the attached document is proprietary to Esri and contains commercial or financial information or trade secrets that are confidential and exempt from disclosure to the public under the Freedom of Information Act. This information shall not be disclosed outside of Customer's organization (except for consultants under a confidentiality obligation who are involved in the proposal evaluation process) without Esri's prior permission, and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this proposal. If, however, a contract is awarded to Esri as a result of this information, the Customer shall have the right to duplicate, use, or disclose the data to the extent provided in the contract. This restriction does not limit the Customer's right to use information contained in this data if it is obtained from another source without restriction.

Attachment D

TECHNICAL PROPOSAL – CH16012 – Cloud Solutions

Esri Proposal to State of Utah and NASPO ValuePoint RFP Solicitation Number CH16012 Master Agreement for Cloud Solutions

Prepared for:

Christopher Hughes, Assistant Director

State of Utah, Division of Purchasing
3150 State Office Building, Capitol Hill

Salt Lake City, Utah 84114-1061
Phone: 801-538-3254

E-mail: christopherhughes@utah.gov

March 10, 2016

Esri Proposal # P16-16115

380 New York Street
Redlands, California 92373-8100 USA
T 909 793 2853

Table of Contents

1.0 RFP Signature Page *

*An electronic version of this document has been submitted separately.

DocuSign Envelope ID: 548A81EE-54BC-488E-8D12-1590C1A97D1D

State of Utah Vendor Information Form

Legal Company Name (include d/b/a if applicable)	Federal Tax Identification Number	State of Utah Sales Tax ID Number	
Esri, Inc.	95-2775732;	12051330-002-STC	
Ordering Address	City	State	Zip Code
380 New York Street	Redlands	CA	92373
Remittance Address (if different from ordering address)	City	State	Zip Code
Esri, File #54630	Los Angeles	CA	90071
Type ☐ Proprietorship ☐ Partnership ☐ Government ☒ For-Profit Corporation ☐ Non-Profit Corporation	Company Contact Person: Doug McColeman		
Telephone Number (include area code): 909-793-2853	Fax Number (include area code): 909-793-5953		
Company's Internet Web Address: www.esri.com	Email Address: info@esri.com		

Offeror's Authorized Representative's Signature
DocuSigned by:
William C. Fleming
BA4744D77EDE442...

Type or Print Name: William Fleming

Position or Title of Authorized Representative: Managing Business Attorney

Date: 3/8/2016

12/15/2014

2.0 Executive Summary

Esri is pleased to provide the attached response to the NASPO ValuePoint Cloud Solutions solicitation #CH16012. Esri views the Master Agreement for cloud solutions as a visionary approach to improving the business of government and its cloud computing practices. With more than 26,000 government organizations worldwide, we are conscious of the challenges NASPO partners face as they work to meet current and future computing needs while containing costs.

Our proposal outlines an affordable, scalable approach for implementing cloud-based GIS in government. We view this Cooperative Purchasing Program as an opportunity to support NASPO participants with cloud GIS infrastructure that not only supports the required business objectives outlined in the RFP but also provides a platform that supports rapidly evolving GIS needs. We believe cloud-based GIS services have the potential to transform how state governments access and manage their GIS resources.

Our proposal response includes ArcGIS Online, Esri's Software as a Service, Esri Managed Cloud Services platform bundles to deliver Esri's ArcGIS platform as a service, and Self-Service Cloud Environments. We also offer a broad range of services to support the configuration and implementation of our proposed offerings.

The proposed approach will allow NASPO participants to:

- Rapidly support SaaS GIS needs and requirements as outlined by NASPO.
- Leverage existing investments in geospatial technology and data.
- Take advantage of new GIS capabilities delivered automatically as the platform evolves, with limited time and resource investments.
- Benefit from Esri's own experience and the experiences of its large customer base in using the ArcGIS platform.
- Leverage the 'interconnected' global framework of cloud infrastructure to integrate with and utilize other cloud- and web-based deployments of GIS content, services and capabilities.
- Choose from a comprehensive collection of hosting services, implementation support and software licensing options that address both cost and service level objectives defined by NASPO.

Our proposed solution has been designed to allow NASPO agreement participants to leverage the cost benefits offered by the Master Agreement while continuing to benefit from their existing licensing agreements with Esri. In support of this effort, we have an established business processes and a focused team to support and manage the NASPO contract exclusively, which was implemented as part of our prior award of the WSCA contracting agreement.

Approach

Esri works closely with our government partners, including members of NASPO, to understand the use and growth of GIS across their organizations and related business needs and challenges. Through this collaboration, we have seen that our customers need to remain agile to adapt quickly to new business priorities while contending with growing resource constraints. We are seeing customers increasingly shift their use of GIS to the web, relying on intelligent web maps as the interface to geospatial applications for both GIS specialists and non-specialists who need access to geospatial analysis and capabilities. In response, we have evolved our commercial software to address these requirements and have established cloud offerings designed to meet varying levels of GIS needs and IT infrastructure maturity. These offerings include GIS and general cloud hosting services to deploy and support ArcGIS in cloud environments and Esri's own integrated cloud-based technology platform, ArcGIS Online.

GIS and General Hosting Services

Purchasing Entities who sign a Participating addendum with Esri will have the option to implement ArcGIS on cloud infrastructure through multiple implementation offerings. The approach leveraged by individual entities will depend on organizational requirements and business needs. The Esri cloud offerings include:

- **Managed Cloud Services Bundles** provide participants with a series of service offerings and a one-stop buying experience for deploying and monitoring Esri software. These Commercial-off-the-shelf (COTS) offerings include a preconfigured deployment of ArcGIS technology with all account management and technical support handled by Esri.
- **Self-Service Cloud Environments** represent a series of offerings that provide a supported computing environment for running Esri software, providing NASPO partners with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, and scalability requirements are the responsibility of the user. We will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

NASPO participants want to use GIS cloud hosting services to reduce costs and gain operational efficiencies such as 24x365 monitoring and technical support for software applications, databases, infrastructure, and other components that uphold critical business processes. Esri can do this. We have provided GIS hosting services since 1997 to many federal, state, and local government customers and have included offerings within this proposal to meet the varying levels of requirements by our government customers.

In support of this effort, Esri continues to work closely and in coordination with government and research groups in the establishment of security guidelines for cloud implementations such as FISMA and FedRAMP. Esri has a proven track record successfully meeting these standards as evidenced by our work implementing FISMA certified solution for both Geospatial One Stop and the geospatial components of Recovery.gov. Esri software is currently running on

Microsoft, Amazon and Terremark cloud environments all of which are in varying levels of compliance with the requirement to host applications in a government cloud infrastructure certified under FISMA, ISO 27001, and SAS 70.

ArcGIS Online

In addition to providing access and consulting support for ArcGIS on public cloud infrastructure, we are proposing an ArcGIS Software as a Service product, ArcGIS Online. ArcGIS Online is a cloud-based geospatial content management system for storing and managing maps, data, and other geospatial services. It is optimized specifically for GIS hosting.

ArcGIS Online is part of the ArcGIS system. It complements all NASPO partners' existing enterprise GIS infrastructures while also providing a rich set of tools, hosting capabilities, and applications to store, manage, and host mapping services. ArcGIS Online also allows users to easily publish geographic content for use within and beyond the organization.

The ArcGIS Platform effectively provides both GIS Software as a Service and a geospatial Platform as a Service (PaaS). It does not require separate infrastructure. By implementing ArcGIS Online, NASPO partners can immediately leverage the following major components: Content Management, Content Publishing, Work Anywhere, Executive Access, Public Access, Collaboration and Workflow Management, Catalog and Data Discovery, Hosted Web Services, User-Generated Web Applications and ArcGIS Online Services.

Conclusion

Esri believes this vehicle provides a unique opportunity for NASPO to transform how state and local governments approach and manage geospatial resources. We have unmatched experience and expertise in providing the geospatial technology, GIS cloud hosting experience, and related services required to meet NASPO’s business needs, and we are prepared to invest the necessary resources to achieve this vision.

Through the combination of offerings, flexible licensing models, and special contract pricing, we are confident that we can offer NASPO a reliable, scalable, and affordable platform to meet current and future requirements. With these offerings, participants can rapidly implement a Cloud based GIS vision. As the leading GIS provider for the majority of NASPO state, city, and county participants, we look forward to continuing to collaborate with all NASPO partners to help support better government for all.

The following sections of the proposal are to be considered business confidential and are not to be made public pursuant to the attached claim of business confidentiality (Attachment A).

- Audited Financial Information, provided under separate cover; Dun and Bradstreet #
- Cost Proposal containing the hourly rates
- Section 4 – Scope of Experience including project experience

3.0 Mandatory Minimums

Response to 5.2 (M) Cover Letter

The rest of this page intentionally left blank.

March 10th, 2016

Christopher Hughes, Assistant Director
State of Utah, Division of Purchasing
Email: christopherhughes@utah.gov
T: (801) 538-3254

Subject: Response to RFP CH16012 – NASPO Value Point Master Agreement for Cloud Solutions

Dear Mr. Hughes,

Environmental Systems Research Institute, Inc. (Esri) would like to thank NASPO for this opportunity to provide a response to your RFP for a Master Agreement for Cloud Solutions.

Esri understands that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

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

Esri 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.

Esri's has SaaS, PaaS, and IaaS offerings to support Purchasing Entity's deployment of cloud GIS.

Esri Cloud GIS Offerings are capable of storing and securing Low Risk and Moderate Risk data:

- ArcGIS Online is capable of storing Low Risk data. ArcGIS Online has been granted FISMA Low ATO by the USDA
- Esri Managed Cloud Services is capable of storing Moderate Risk Data. Esri Managed Cloud Services has been granted FedRAMP Moderate ATO by the US Census Bureau.

This proposal will remain fixed and valid for a 90 day period from the Due Date of March 10th, 2016.

We look forward to working with NASPO on this contract and if you have any questions, please do not hesitate to reach out to us.

Sincerely,

John D. Perry
Contracts Manager, Professional Services
Ph: (909) 793-2853 x1133
Email: jperry@esri.com

380 New York Street
Redlands, California 92373-8100 USA
909 793 2853
info@esri.com
www.esri.com

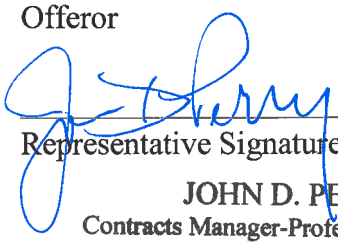
Response to 5.3 (M) Acknowledgement of Amendments

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

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

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

Environmental Systems Research Institute, Inc. (Esri)
Offeror



Representative Signature

JOHN D. PERRY
Contracts Manager-Professional Services

Response to 5.5 (M) General Requirements

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

Esri agrees that it will provide a Usage Report Administrator for this agreement.

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

Esri agrees that it will cooperate with NASPO ValuePoint and its authorized agent with uploading ordering instructions, if awarded a contract.

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

Esri is providing the following as part of attachment B, Exhibit 2 (see Appendix A).

- Esri's GIS SaaS offering, ArcGIS Online: Completed Cloud Controls Matrix (CCM) questionnaire.
- Esri's GIS PaaS offering for Managed Cloud Services Bundles – Esri Managed Cloud Services (EMCS). Completed Cloud Controls Matrix (CCM) questionnaire.
- Esri's IaaS offering – Self-Service Cloud Environments. As described in Section 8.1.3, Esri's offering also includes Self-Service Cloud Environments (IaaS). This offering uses Amazon Web Services (AWS) cloud infrastructure. The AWS CSA CAIQ questionnaire is published on the AWS compliance site at the following location:

  https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

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

Please see Section 8.4.1 for a description of a sample Service Level Agreement

Response to 5.7 Recertification of Mandatory Minimums and Technical Specifications

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

Esri acknowledges that it will certify with the State of Utah on an annual basis, to reconfirm that we still meet or exceed the technical capabilities discussed.

4.0 Business Profile

Response to 6.1 (M) (E) Business Profile

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

Esri develops GIS software that helps organizations deliver effective and sustainable solutions to problems around the world. We offer ArcGIS, a complete location platform that lets users create maps and location apps and share them with anyone who needs them, anywhere, and on any platform or device. We also provide user education and training, technical support, and professional services to help our users apply our technology to make more effective decisions and improve outcomes.

Our Capabilities

Founded in 1969, Esri is a financially stable, privately owned corporation with a policy of zero debt. Private ownership means no stockholders forcing short-term decisions at the expense of long-term objectives. This lets us maintain a strong commitment to innovation and rapidly address the changing and emerging needs of our user community. Each year, we reinvest more than 27 percent of our revenue in research and development to support new advancements in our platform technology.

To help our users effectively implement geospatial technology to meet their needs, Esri maintains a global partner network of more than 1,800 partners, including strategic alliances with major technology leaders such as Amazon Web Services, IBM, Microsoft, SAP, and SAS. We also have more than 80 international distributors that support Esri users in more than 150 countries.

Our Customers

Esri is dedicated to helping customers use geospatial technology to solve their unique operational challenges. By listening closely to the people who use our software every day, we receive valuable user feedback and recommendations that we incorporate in our product releases. As a result of this commitment to fulfilling the needs of our customers, our platform has become widely pervasive and supports users in many industries.

Today, Esri software is used by more than 350,000 organizations worldwide including:

- Most US federal and national mapping agencies
- All 50 US state health departments
- Each of the 200 largest US cities
- More than 24,000 state and local governments worldwide
- More than two-thirds of Fortune 500 companies
- 45 of the top 50 petroleum companies
- More than 7,000 colleges and universities
- Many others in dozens of industries

Esri has provided online services since 1997 to many federal government, state and local government, and commercial customers. Esri's online services offerings began as data services to support a variety of commercial and government GIS solutions. Our work providing online services has progressed to include managed services including IaaS, PaaS and SaaS offerings. Esri is the world leader in delivering complete GIS solutions like political redistricting, Business Analyst, Community Analyst, ArcGIS.com and ArcGIS Online. Our experience includes not only the development and deployment of integrated online capabilities but also the business processes and third party management required to provide viable solutions as part of the core ArcGIS capabilities.

Esri has been a Cloud Services provider to the Western States Contract Alliance (WSCA) and NASPO since 2012 and has completed projects under this contract for the State of Hawaii and State of Washington.

Response to 6.2 (M) (E) Scope of Experience

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

Esri has provided online services since 1997 to many federal government, state and local government, and commercial customers. Esri's online services offerings began as data services to support a variety of commercial and government GIS solutions. Our work providing online services has progressed to include Managed Cloud Services associated with IaaS, PaaS and SaaS offerings. Esri is the world leader in delivering complete GIS solutions like political redistricting, Business Analyst, Community Analyst, and ArcGIS Online. Our experience

includes not only the development and deployment of integrated online capabilities but also the business processes and third party management required to provide viable solutions as part of the core ArcGIS capabilities. The following are five examples of government and large organizations that we have worked with over the years to provide support and management their geospatial platforms.

Please see Section 7.0 for a list of past projects, which are to remain confidential.

Response to 6.3 (M) Financials

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

Esri remains financially strong with zero debt, growing market share, and above-average growth for a global IT company.

Our GIS technology is primarily focused on managing, analyzing, applying, and presenting geographic data. In addition, a multibillion-dollar industry has developed around our products as other companies augment our technology or apply our tools in specialized applications and workflows. This growth is happening at an even faster rate than the growth of our core platform technology. Furthermore, because GIS technology is migrating to the web and to mobile devices like tablets and smartphones, we expect to see exponential growth in the next several years.

As a private corporation, Esri's financial statements are not published or readily available to the public. However, pursuant to the State of Utah Business Confidentiality agreement, Esri has provided a copy of its audited financials under separate cover to Mr. Christopher Hughes in compliance with the requirements of this section.

Please see Section 7.0 for Esri's Dun and Bradstreet #, which is to remain confidential.

Response to 6.4 (E) General Information

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

As cloud technologies have matured, Esri's portfolio has evolved to meet the changing needs of the marketplace. 10 years ago, our cloud offering was limited to hosting applications for our customers. Today Esri offers a full range of cloud offerings, from reselling infrastructure on behalf of our cloud partners, to an Enterprise-ready platform which can be used to build and

share maps and apps, to a fully-supported SaaS offering. These offerings have been implemented for hundreds of clients looking to cloud-enable their GIS practices. Additionally, we recognize cloud adoption is often a journey and we have developed a number of value added services designed to assist our customers regardless of their comfort with cloud technologies and regardless of whether their ultimate aim is DIY cloud or a fully-managed implementation of Esri's ArgGIS platform.

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

Esri's cloud GIS offerings utilize infrastructure from Amazon Web Services and Microsoft Azure. These cloud infrastructure providers have auditing capabilities and reports that are consistent with SSAE16 6/2011 or greater. In addition, the government authorizes ArcGIS Online as FISMA Low compliant and EMCS as FedRAMP moderate compliant. FISMA and FedRAMP auditing and reporting are significantly more robust then SSAE audit/reports.

Response to 6.5 (E) Billing and Pricing Practices

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

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

Esri's offer includes managed services (cloud/hosting) as well as consulting services offered as packaged products and at hourly rates. The type of order, firm fixed price or time-and-materials, will determine the invoice format and content. Invoices are prepared in accordance with contract terms and generally are prepared on a monthly basis. The following invoicing details are provided for each order type:

Firm Fixed Price Orders

- Managed Services are typically invoiced monthly based on the negotiated pricing in the order. Invoice includes:
    - Hosting Service Period being invoiced
    - Products invoiced as outlined in client order
    - Contact information for questions
- Consulting Packages are typically invoiced in full at the time the order is placed. Packages expire without refund if not expended within 12 months Invoice includes:
    - Product invoiced as outlined in client order
    - Contact information for questions

Time-and-Materials Orders

- Consulting services provided under this order type will be invoiced monthly as work is performed. The invoice will include:
    - Period of performance being invoiced
    - Details on labor hours and labor rates expended
    - Details on travel or other non-labor costs
    - Contact information for questions

In addition, Esri typically provides formal or informal progress reporting if requested.

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

The primary cost drivers for cloud solutions can be classified into three basic categories: Users, Size, and Services Offered.

Users

Whether describing named users, administrators, or public viewers, the number of users and their roles play an important part in the size and type of solution which should be implemented.

Size

Purchasing Entities should consider the size and type of their data set when planning on costs. Larger data sets typically require more storage and would incur higher costs.

Services Offered

The majority of services run on the ArcGIS platform require roughly similar workloads of the server. However, there are a few specialized services which put incremental loads on the infrastructure and should be noted when considering costs, specifically: Geocoding, image processing, big data analytics, and large batch processing.

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

Please see section 8.1.2 for a description of how Esri solutions are NIST compliant as defined by NIST Special Publication 800-145.

Response to 6.6 (E) Scope and Variety of Cloud Solutions

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

Esri develops GIS software that helps organizations deliver effective and sustainable solutions to problems around the world. We offer our solution through the ArcGIS platform, a complete location platform that lets you create maps and location apps and share them with anyone who needs them, anywhere, and on any platform or device.

Our ArcGIS platform is available as software as a service (SaaS) through ArcGIS Online, as a platform as a service (PaaS) with ArcGIS for Server plus a Managed Service product offer, or customers may provision infrastructure as a service (IaaS) necessary to support the ArcGIS platform through Esri. Regardless of the type of service (IaaS, PaaS, SaaS), Esri's solutions would be classified as GIS.

ArcGIS Online (SaaS)

Esri's secure, multitenant cloud that's scalable and ready to use. No additional hardware or software has to be purchased or installed. ArcGIS Online gives users in a Purchasing Entity's organization access to tools, basemaps, and other content to make and share maps and applications. Users can catalog and discover maps and applications; set up groups to collaborate; and share items with each other, the entire organization, or publicly. For example, without any programming, any user that's part of an ArcGIS Online organizational account can quickly share maps by embedding them in a website or blog, through social media, or by using preconfigured web application templates.

ArcGIS for Server (PaaS)

Purchasing Entities have the ability to procure the ArcGIS platform through the Esri Managed Cloud Services team. The Managed Cloud Services bundles are designed to grant Purchasing Entities access to all of the features of ArcGIS for Server including Portal while removing the responsibilities normally associated with administering the Platform. By purchasing a Managed Cloud Service bundle, Purchasing Entities gain access to Esri's cloud and GIS expertise. This partnership allows a Purchasing Entity's resources the freedom to focus on delivering location value with the confidence that Esri will deliver a system to support its strategic and operational goals.

Self-Service Cloud Environments

For Purchasing Entities interested in deploying GIS in the cloud on their own, Esri offers Self-Service Cloud Environments. By subscribing to a Self-Service Cloud Environment, Purchasing Entities have the ability to self-provision infrastructure resources on-demand. Self-Service Cloud Environments serve as the gateway for cloud-enabled GIS, giving Purchasing Entities access to

administration tools which allow for self-provisioning of cloud application(s), servers to support GIS and database needs, as well as storage capacity. Purchasing Entity resources will have the ability to select from a variety of cloud infrastructure providers and can select their operating systems, database management systems, and Esri ArcGIS technologies of choice. Purchasing Entity's representatives are responsible for provisioning new servers, storage, databases, and any other infrastructure required as well as deploying and managing software. The representatives may choose to set up remote access to provisioned servers and are therefore free to deploy and modify databases on demand. Upon task order award, Esri will engage with the infrastructure partner ("Infrastructure Host") selected by the Purchasing Entity to activate a dedicated cloud self-service account for the Purchasing Entity.

Once an Environment is provisioned, the Purchasing Entity has the ability to load data, publish web services, deploy web applications and take advantage of other cloud administration tools, such as elastic load balancing and auto-scaling. It is the Purchasing Entity's responsibility to provision, administer and manage the Environment in accordance with their desired security and operational standards. There is no Service Level Agreement associated with data, services, or applications hosted with Self-Service Cloud Environments. Organizations can use existing ArcGIS for Server licenses or choose from convenient, renewable, 1-, 3-, and 12-month term licensing.

Response to 6.7 (E) Best Practices

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

Policies and procedures of Esri's Cloud Hosting offerings that are generally aligned with NIST 800-53 controls and satisfy FISMA Low or FedRAMP moderate requirements. Esri's Cloud Hosting offerings utilize physical infrastructure provided by Amazon Web Services (AWS) and Microsoft Azure whose policies and procedures align with ISO 27001 and FedRAMP Moderate.

Esri practices to secure data and applications hosted in our cloud systems focus on minimizing potential attack surfaces and on continually monitoring information systems to detect and mitigate potential vulnerabilities. Esri uses independent 3rd party auditors for our Cloud GIS offerings in compliance with FedRAMP Moderate sensitivity for Esri Managed Cloud Services (EMCS) which is Esri's PaaS Cloud hosting environment and FISMA Low for ArcGIS Online.

Managed Cloud Services Bundles (PaaS/SaaS)

Esri Managed Cloud Services (EMCS) includes policies and procedures for authentication and authorization. EMCS supports integration with SAML 2.0 compliant identity providers (IdPs) to ensure users can leverage existing authentication mechanisms as well as existing organization-approved policies, procedures, and processes for account provisioning. Authorization is based

on roles which define what a specific user can see. For EMCS administrators, EMCS enforces strong password policies and two-factor authentication for administrators accessing those environments. Please see Section 8.6.7 for additional details.

Less than 10 Esri personnel have access to EMCS, and privileges are assigned based on role and using the principle of least privilege. Prior to accessing a Managed Cloud Services bundle, all employees must acknowledge and sign a Rules of Behavior (RoB) that outlines technical and organizational responsibilities related to the access and use of EMCS. For additional details, please see Section 8.6.4.

The confidentiality and integrity of customer data at rest is protected by implementing encryption of data sets (file servers and databases) using AES-256 FIPS 140-2 compliant encryption. EMCS only permits connections on port 443 to FIPS 140-2 compliant end-points Customers and EMCS Administrators must connect to EMCS infrastructure using TLS only. Administration and Infrastructure keys are managed through key management which aligns with FedRAMP Moderate security requirements. Please see Section 8.5.1 and 8.6.3 for additional details.

For compliance, EMCS employs a continuous monitoring plan which includes security control reviews to ensure effectiveness. EMCS is designed and developed to be a hardened environment that limits exposed services and minimizes potential attack surface. Automated scanners and manual testing are performed against application and programming interfaces to align with industry standards such as OWASP. This is a mandatory requirement as part of FedRAMP Continuous Monitoring and ensures potential threats are identified, tracked and mitigated to provide constant security assurance. A full security control review is conducted annually along with a vulnerability assessment and penetration testing to ensure compliance. Please see Section 8.6.5 and 8.6.6 for additional details.

A third-party audit by approved, independent FedRAMP auditors is done annually to ensure accountability. This ensures the appropriate technical and organizational measures are in place to provide customers with the assurance that their data is protected.

ArcGIS Online (SaaS)

ArcGIS Online includes policies and procedures for authentication and authorization. ArcGIS Online supports integration with SAML 2.0 compliant identity providers (IdPs) to ensure users can leverage existing authentication mechanisms as well as existing organization-approved policies, procedures, and processes for account provisioning. Authorization is based on roles which define what a specific user can see. ArcGIS Online allows users to set strong password policies. Please see Section 8.6.7 for additional details.

Less than 10 Esri personnel have access to ArcGIS Online, and privileges are assign based on role and using the principle of least privilege. Prior to accessing ArcGIS Online, all employees

must acknowledge and sign a Rules of Behavior (RoB) that outlines technical and organizational responsibilities related to the access and use of EMCS. For additional details, please see Section 8.6.4.

ArcGIS Online data protection controls align with FISMA Low sensitivity. ArcGIS Online provides system administrators of Participating Entities with the option of requiring encryption in transit via HTTPS (TLS) for data transmitted to and from their ArcGIS Online organization. ArcGIS Online does not encrypt customer data at rest. However, a Participating Entity may choose to encrypt their data either through their application or by leveraging an enterprise cloud encryption gateway solution. Customers with data sensitivity concerns frequently choose to implement a hybrid solution where sensitive data is kept on premises or in a separate cloud with higher security measures, such as Esri's EMCS offering as described above. Please see Section 8.5.1 and 8.6.3 for additional details.

ArcGIS Online releases which include patches and bug fixes are performed quarterly. If security vulnerabilities are found or reported, they are assessed by the ArcGIS Online Leads, and fixed. Any vulnerabilities that have an assessed risk of high or critical are patched immediately outside of normal patching routines. ArcGIS Online vulnerability management aligns with FISMA Low requirements and includes continuous monitoring to ensure any issues are resolved within defined timelines commensurate to assessed risk level. Please see Section 8.6.5 and 8.6.6 for additional details.

Continuous monitoring includes vulnerability assessments and security control reviews. ArcGIS Online utilizes third party auditors as part of FISMA Low compliance.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, and scalability requirements are the responsibility of the user. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

Physical cloud infrastructure can be provided by Amazon Web Services (AWS) and aligns with ISO 27001 and FedRAMP Moderate. For more information on their compliance information, see Amazon Web Services (https://aws.amazon.com/compliance/).

5.0 Organization Profile

This Section focuses on the individual persons and roles that will be involved in performance of the Master Agreement. The State has identified a number of roles that are necessary based on the requirements of **Attachment D**; these titles are not meant to be restrictive, but are used to identify key roles. The State recognizes that different Offerors may use different titles, have different organizational structures, and employ roles that have not been specifically identified by the State. For the roles that have been identified, provide the required information about the person/role that will meet the requirements identified by the State; feel free to provide the title your business uses for that role. If multiple identified roles are performed by the same person, be sure to include that information in your response.

Response to 7.1 (M) (E) Contract Manager

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

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

For almost 15 years, Esri has been providing managed hosting services to many successful clients across the State, Local, and Federal Government levels.

To support the NASPO contract, Esri will utilize its Corporate Accounts team and Professional Services Contracting team, with a designated NASPO contact, to act as the dedicated NASPO Contract and Usage Reporting Administrator. Combined, these teams have over 15 years of experience managing Esri's hosting services business.

The Esri NASPO Contract Administrator will have full authority to enforce the scope of work and terms and conditions of the resultant contract, and will be supported by a team of cross-trained professionals with the capability of assisting them as well as participating NASPO entities with usage reporting to support quarterly and annual sales reporting as outlined in the RFP.

The Esri NASPO Contract Administrator and support staff will be responsible for conducting annual and quarterly NASPO account reviews as well as meetings with individual entities. This team will be prepared to provide each with the following information:

- Quarterly usage report for each customer that includes type of usage by month
- Cost structure summaries for each entity
- Issue tracking and responses review

- Review of new cloud technologies and business infrastructure improvements and provision of recommendations for adoption
- Review of security, FISMA, government compliance and specific organization requirements
- Measure of contractors' performance with specific metrics as identified by NASPO and Cloud Hosting Provider

The Contract Administrator will work with NASPO and Participating Entities on the scope and specific reporting requirements upon contract award. Please contact Robin Espinoza, the Contract Administrator, at (909) 793-2853 x3918, for more information.

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

Robin Espinoza is a Senior Contracts Administrator within the Professional Services group. She has extensive experience managing the various WSCA engagements specifically for the State of Hawaii and Washington. She was also a key contributor to drafting the contractual provisions for the prior WSCA contract as well as for this response. In addition to managing the WSCA engagements on the prior contract, Mrs. Espinoza also is a senior level contracts administrator, well versed in negotiation of all aspects of services contracting for state and local government entities. She currently manages several large complex contracts for some of the Division's largest clients. See below for a resume for Ms. Espinoza.

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

In addition to the details outlined above, Robin will be responsible for review and execution of all participating addendums with ordering entities throughout the life of the contract. She will actively review all scope and pricing and additional ordering terms, and negotiate with the respective entities as required. She will also interact with the Corporate reporting function to ensure that all required reports are prepared and submitted correctly and on time.

Robin Espinoza

Sr. Contracts Administrator

Career Highlights

- Manage complex contracts for GIS services for state and local entities
- Handle all cloud hosting engagement addendums in support of WSCA Cloud computing.
- Experienced Negotiator of all Key Contracting terms – price, quality, licensing, penalties, intellectual property provisions
- Expertise with a wide variety of industries including Defense, Commercial, medical device, industrial automation, GIS consulting

Experience

Esri: 6 years

Total: 27 years

Education

- MS (Organizational Management), University of Phoenix, Phoenix, AZ, 1994
- BS (Major): Business Administration/Marketing, Northern Arizona University, Flagstaff, AZ, 1984

Selected Experience

Senior Contracts Administrator, Esri Professional Services, 2010-Present

- Handle all cloud hosting engagement addendums in support of WSCA Cloud computing.
- Management of Division's largest local government client, contract work in excess of $10M, with over 22 active subcontractors
- Negotiate complex IP provisions including IP Ownership, Limitation of Liability, Terminations with key strategic clients
- Responsible for contractual negotiations of Master Purchase Agreements/Service Agreements for all 50 states.
- Team with Corporate to negotiate favorable contracts for state clients relating to professional services (T and M) / FFP efforts
- Favorably resolve complex contract issues such as payment, acceptance, Termination settlements for key client base

Senior Sourcing Manager, Medtronic Microelectronics Center, 2007-2010

- Managed major subcontracts for custom medical implantable components in France, Singapore
- Conducted high level negotiations to achieve $3.0M cost down per year
- Developed and Monitored International Contracts for custom electronic and electro-Mechanical components worth $30M annually
- Developed and executed commodity strategies for high impact commodities including custom semiconductors, electromechanical parts, services, plating
  Led Cross Functional team to implement process improvements related to incoming inspection with a yearly savings of $1.0M upon implementation

Employment History

Employer	Position Title	Position Dates
Esri	Senior Contract Administrator	2010–Present
Medtronic Microelectronics	Senior Sourcing Manager	2007 - 2010
Honeywell International	Supply Chain Manager Manager, Global Strategic Sourcing Commodity Buyer/Planner	2005 – 2007 1999 – 2005 1998 - 1999
Motorola Tactical Electronics Division	Buyer / Senior Buyer	1989 - 1998

6.0 Technical Response

In preparing our response to this RFP, Esri has considered our past experience providing cloud solutions to our customer base, current trends in cloud, and has attempted to craft an offering that will continue to satisfy organizations' business, technical, and security needs into the future. Our experience is that every organization has unique needs and missions and we measure success in terms of our clients' ability to meet their needs and deliver on their missions. The ArcGIS platform has played a central role in our clients' ability to deliver valuable location insight for more than 40 years and we are committed to helping our clients get value from GIS well into the future. To this end, Esri offers solutions through each cloud service model (IaaS, PaaS, and SaaS). By offering services across the service model spectrum, every organization may choose the platform implementation that best suits its needs.

As the market leader in GIS, Esri has played a key role in the technological shifts in GIS of the past 40 years. Esri has helped companies as they have shifted their GIS practices from mainframes to personal computers, from PCs to servers, and we've been engaged in helping our clients adopt the cloud for the past 10 years.

Our response reflects the latest in our cloud offerings and the best GIS cloud offerings on the market. In support of this effort, Esri continues to work closely and in coordination with government and research groups in the establishment of security guidelines for cloud implementations such as FISMA and FedRAMP. Esri has a proven track record successfully meeting these standards as evidenced by our work implementing FISMA certified solution for both Geospatial One Stop and the geospatial components of Recovery.gov as well as receiving our FedRAMP Moderate - Authorization to Operate from the US Census Bureau in support of its Business Builder initiative.

Response to 8.1 (M) (E) Technical Requirements

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

Esri provides cloud offerings that meet the definition of Platform as a Service (PaaS) and Software as a Service (SaaS). Esri also resells Infrastructure as a Service (IaaS) in support of cloud-based GIS projects. Esri's SaaS offering is deployed on the public cloud; the PaaS offering can be deployed in the public, community, or hybrid cloud; the deployment models supported by the IaaS offering depends on the Infrastructure Host selected by the Purchasing Entity.

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

Esri strives to continuously advance the capabilities of our products to meet customer demands, including capabilities that help us improve our alignment with the essential characterizes on cloud computing as defined by NIST 800-145.

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

The Managed Cloud Services Bundles provide different support models for on-demand deployment. With the Small bundle Esri will provision the servers, but the Purchasing Entity is responsible for any new software deployments to their provisioned servers. The Purchasing Entity's representative is provided with an administrator account to the operating system to support this. With the Medium, Large, and X-Large bundles Esri manages the deployment of all software, and can support on-demand deployment 24x365.

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

A Purchasing Entity can access resources through broad network access using a variety of devices such as laptops, mobile devices, tablets, etc. for all of Esri's proposed IaaS, PaaS, and SaaS offerings. For the Self-Service offering a Purchasing Entity has the ability to provision resources over the internet from just about any location that has adequate network connectivity. This applies to the Esri Managed Cloud Services offerings where access to managed resources will be provided over the internet to users who are authorized.

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

Through the Self-Service Cloud Environments offering Esri supplies users with access to cloud resources that can come from a variety of cloud providers and include a variety of cloud services (compute, storage, bandwidth, etc.). Purchasing Entities can select from a number of these services and provision dynamically depending upon demand. If desired, they can also select the geographic location of where these dynamic resource reside.

Through Esri Managed Cloud Services a Purchasing Entity will engage with Esri cloud architects to determine their specific needs. Based on that, Esri will setup an environment based on the appropriate service level selected and/or recommended. Resources such as compute,

storage, bandwidth, etc. will be provisioned by Esri and can be added or removed depending upon demand.

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

One of the options for Self-Service Cloud Environments is currently based on infrastructure provided by Amazon Web Services (AWS). In this offering the customer has direct access to the AWS Management Console, which can be used to scale up and scale down 24x365. New instances may be added in one hour or less. With these offerings it is the customer's responsibility to scale up and scale down. When provisioning GIS systems based on ArcGIS 10.1 for Server, the Participating Entity may also leverage the ArcGIS for Server Cloud Builder software made available by Esri to facilitate both manual and automatic scaling of ArcGIS for Server software.

The Managed Cloud Services Bundles provide different support models for scaling up and down infrastructure.

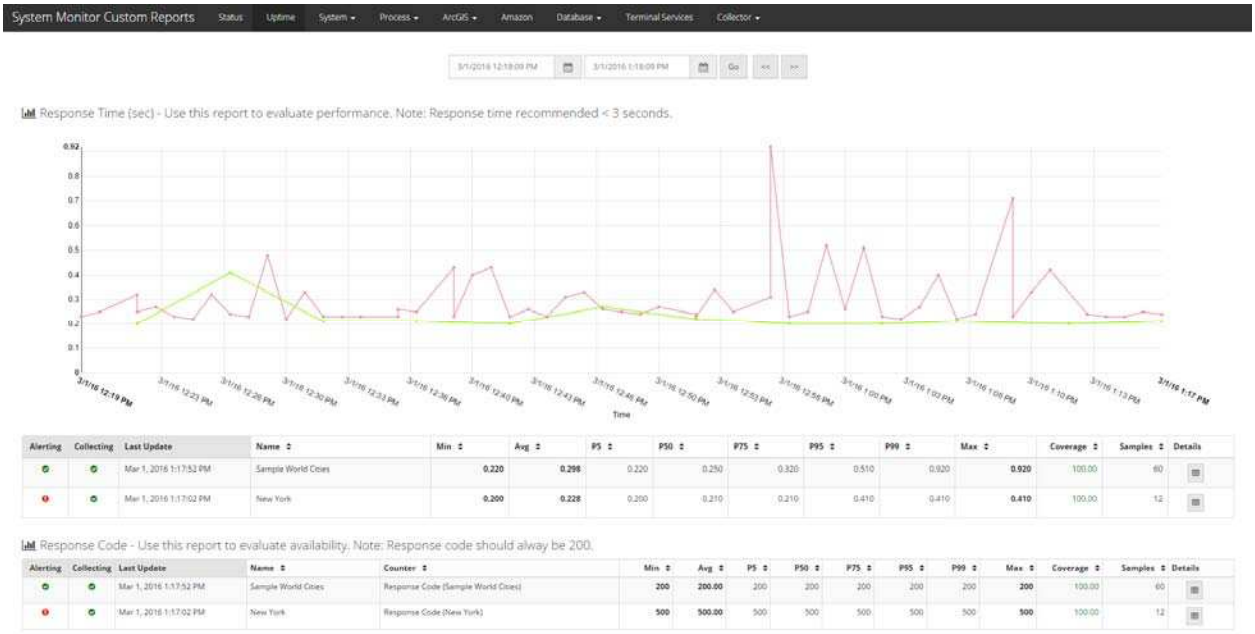
With the Small bundle Esri manages the provisioning and de-provisioning of infrastructure. At the request of the customer, Esri can provision (i.e. scale-up) and de-provision (i.e. scale-down) infrastructure. The provisioning of infrastructure may require new task orders, and therefore may be subject to the terms and schedule of the NASPO contract administration process.

The Managed Cloud Services Medium, Large, and X-Large bundles include auto-scaling. The auto-scaling service allows for the dynamic scaling of server resources to address high demand on infrastructure resources. This service not only allows the rapid deployment of new server resources but also removes servers when they are no longer needed, eliminating unnecessary costs associated with excess capacity.

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

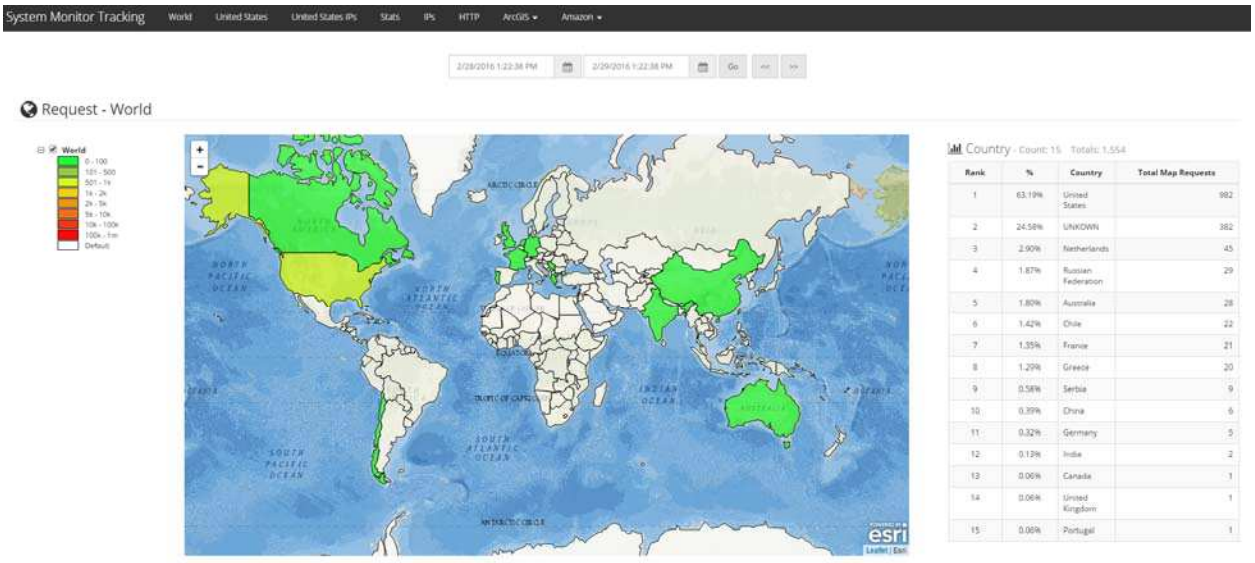
When a Purchasing Entity engages with Esri through Self-Service Cloud Environments they will be given direct console access to cloud resources. They will be able to view through monitoring tools the amount of resources that are being consumed.

Through the Managed Cloud Services Bundles the Purchasing Entity will be provided with access to reports showing additional metrics on usage of their GIS systems. Esri has developed custom reporting and monitoring tools tailored to support its products. Below is a screenshot of a sample report showing system uptime:



System Uptime

The screenshot below is an example report showing where requests are coming from globally and how many:



Global Requests

Custom reports can be configured to meet the Purchasing Entity's needs under the Esri Managed Cloud Services offerings.

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

ArcGIS Online, Esri's SaaS offering is classified as GIS SaaS.

Esri's PaaS offering is classified as GIS PaaS.

Esri's offerings for IaaS are all designed to be deployed in support of ArcGIS and would be classified as GIS IaaS. It is not Esri's intention to be a reseller of IaaS for non-GIS projects.

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

Esri is willing to comply with the requirements of Attachments C & D.

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

Esri's offerings adhere to the services in Attachment D and comply with Public, Community, and Hybrid cloud. Esri Managed Cloud Services supports its customers in public cloud environments such as AWS and Azure, has the ability to support users with managing their geospatial content in Community environments such as AWS GovCloud and has a vast amount of experience in designing customer solutions to run in hybrid environments.

Response to 8.2 (E) Subcontractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

Esri's intent will be to provide all cloud solutions directly without subcontracting work to subcontractors. However, Esri does maintain a vast number of Business Partners that can be leveraged to provide services on an as-needed basis. Esri will work with NASPO and the State of Utah to review any subcontractors or business partners that might be engaged for future work.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed

description of how the subcontractors are anticipated to be involved under the Master Agreement.

Please see statement above.

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

Esri does not intend to use subcontractors at this time.

Response to 8.3 (E) Working with Purchasing Entities

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

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

Response times;

Processes and timelines;

Methods of communication and assistance; and

Other information vital to understanding the service you provide.

Esri's Cloud GIS systems have security incident response plans that define how security incidents, including data breaches must be handled. The plans define roles and responsibilities, key capabilities, training, and security incident handling process (preparation, detection and analysis, containment, eradication, and recovery, and post incident activities) that must be followed for security related incidents. The security incident response plan includes a combination of procedural and technical elements for the tracking of security-related events from the identification phase all the way through resolution. Please see Section 8.6.8 for additional information on security incident handling procedures.

Upon award of a contract to provision Cloud GIS services Esri and the Participating Entity will review incident response procedures and define the specifics as they pertain to the engagement, including specific contact list for any breach related communications, communication protocols, and timelines.

Esri' standard is to notify the customer of a confirmed breach that impacts a Participating Entity's data or information within 72 hours. This follows the standard established by DFARS

252.204-7012. The communication will be initiated through the through Esri's assigned Contract Manager as defined in Section 7.1, who will then notify the Participating Entity's assigned representative. Technical and operational personnel to be involved will depend on the nature of the breach but will typically include Esri internal security personnel who will work with internal technical resources as well as Participating Entity's representatives as appropriate to resolve the issue. Depending on the nature of the incident, communications may also involve representatives from law enforcement, US-CERT, or Esri's Cloud infrastructure providers.

Additional information pertaining to specific Esri Cloud GIS offerings are provided below.

Managed Cloud Service Bundles (PaaS/SaaS)

EMCS Incident Response policies, procedures and processes are documented in the EMCS Incident Response Plan and align with FedRAMP Moderate requirements. EMCS has a specific communication plan depending on the nature of the incident to ensure proper legal precautions are taken and chain of custody is maintained throughout an incident.

Per standards set in DFARS 252.204-7012 Esri notifies the customer of a confirmed breach that impacts the customer's data or information with 72 hours. As detailed in the EMCS Incident Response Plan, notification, communication and involvement beyond the Participating Entity, Esri and the EMCS ISSO may include: Amazon, Law enforcement, US-CERT, the FedRAMP PMO, and others as necessary. During resolution of the breach, Esri will provide updates to the Participating Entity based upon a mutually agreed upon schedule.

EMCS personnel are required to report suspected security incidents according to the protocols defined in the Incident Response plan within timelines recommended by US-CERT specified in NIST SP 800-61 (as amended).

ArcGIS Online (SaaS)

Security incident management is delineated within ArcGIS Online's Incident response plan documentation which aligns with FISMA Low requirements. Per standards set in DFARS 252.204-7012 Esri notifies the customer of a confirmed breach that impacts the Participating Entity's data or information with 72 hours. Esri will coordinate with appropriate parties to investigate the security breach and will take commercially reasonable steps for remediation based on Esri's assessment of risk. Esri will provide updates to the Participating Entity with applicable information on a mutually agreed upon schedule.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for customers with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, and scalability requirements are the responsibility of the user. Esri will ensure the environment is accessible

and that all appropriate Esri software is available for management and configuration. Security incident handling procedures will be defined based on the specifics of an engagements with a Participating Entity.

Physical cloud infrastructure can be provided by Amazon Web Services (AWS) which includes its own incident response plans and procedures in alignment with ISO 27001. For more information on AWS compliance information, see Amazon Web Services (https://aws.amazon.com/compliance/).

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Esri, as a whole, does not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the State of Utah and will continue to uphold this practice for the duration of the contract.

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

Participating Entities have the ability to purchase environments for testing and staging identical to their production environments. Purchasing Entities purchasing a Self-Service Cloud Environment would be responsible for the configuration of said environments while organizations purchasing a Managed Services Cloud Bundle may opt for a second bundle for testing and staging purposes.

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

Esri's Cloud hosting offerings, ArcGIS Online and Esri Managed Cloud Services (EMCS), provide customers with the GIS capabilities of the ArcGIS Platform in the cloud. The ArcGIS Platform includes Web APIs that can be used to develop applications that are accessible to people with disabilities. Esri has a defined policy on Section 508 compliance, which can be found at the following URL. Esri.com/legal/section508. Voluntary Product Accessibility Templates (VPATs) for the ArcGIS Platform are available at this URL: http://www.esri.com/legal/section508/swguide

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

Esri's SaaS offering ArcGIS Online and Esri Managed Cloud Services provides access to applications and datasets through standard internet browsers such as Internet Explorer, Chrome, Firefox, etc.

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

On an exception basis, if a Participating Entity desires Esri to handle PII that will need to be specified up front by the Ordering Entity. If Esri agrees, there will be a meeting between Esri and the Purchasing Entity to plan how to store and manage that information.

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

Schedules with any Purchasing Entity will be defined upon executing a contract and a timeline for setting up and providing environments for development, testing and production will be determined.

Response to 8.4 (E) Customer Service

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

Quality assurance measures;

Escalation plan for addressing problems and/or complaints; and Service Level Agreement

Esri's customer service and incident response process may vary depending upon whether it is specifically for Esri Products or whether it is related to Esri's Managed Cloud Services offering.

Esri Software Products and SaaS offerings:

Occasionally, a customer encounters an error that is so severe that their business is seriously affected. In these situations, either the customer or an Esri account representative can escalate the case.

When a case is escalated, Esri assigns the most qualified analyst possible within four hours to act as the lead support analyst for the case. Management continues to monitor the case and takes any necessary steps to resolve the case as quickly as possible. Meanwhile, the assigned support analyst follows the normal troubleshooting process while keeping the customer updated every two business days with their findings and the status of the case. To reflect the serious nature of

escalated cases, support analysts who are assigned to these issues will have their work prioritized to focus on the issue until it is resolved or a workaround can be provided.

Defect Escalation

Once an issue has been determined to be a defect in the software, our development teams will evaluate and prioritize the defect so that a fix is applied during the software release cycle. Esri Support Services can escalate a defect to make the fix a higher priority for an upcoming software release.

If a request from a specific customer is made to escalate a defect, the support technical leads will inform the relevant product development lead of the issue and obtain a timeline for the issue's resolution. Support staff will then communicate this information to the customer. Support staff will also regularly inform the customer of the resolution's progress and serve as the liaison for the remainder of the defect's life cycle.

Quick Fix Engineering (Hot Fix)

Sometimes software defects are so critical that they require extraordinary attention and effort to get the customer back on track. First, a business justification must be submitted by the users through their account manager to a technical account manager (TAM) that works in Esri Support Services. The TAM will work with the development team on passing the business justification on for approval. In these rare situations, the issue is forwarded to our Quick Fix Engineering (QFE) team once it is approved. The QFE team then takes ownership of the issue and develops a hot fix, which is a software patch that targets the functional area deemed critical for the customer on a particular version and platform. Hot fixes are delivered with documentation that clearly explains the original issue and how the hot fix resolves the problem. Once they have been developed, hot fixes are typically included in future releases to mitigate any related issues that other customers might encounter.

Esri Managed Cloud Services (PaaS / SaaS)

The following is a summary which describes the processes and procedures that Esri Managed Cloud Services uses to support customer data and applications in a cloud production environment.

Change Management

During the requirements validation phase, the customer is asked whether they will need Esri to apply updates to the application and/or data content after it is officially in production. Changes to production systems will need to be validated and approved by Esri's Change Advisory Board (CAB) prior to being made to the system to comply with best practices. When a customer has identified that a change needs to be made, the customer must fill out the "Change Request Form" which includes information such as the following:

- Description of the change request
- Urgency of request and time the change needs to be in place
- Verification that the changes have been tested in an internal QA environment prior to sending to Esri
- All necessary application configuration files, data content and deployment instructions

Once the above information has been provided, Esri will work with the customer to identify a timeline for the change and assess the level of effort and risk associated with making the change. Low Risk, which are changes with no downtime, can be applied in 24-48 hours upon approval from the CAB. Medium to High Risk changes can be applied in approximately 1 week depending on the complexity of the change and CAB approval. Emergency Changes which are medium to high risk and need to be applied in 24 hours or less will require justification and will be assessed by the CAB. Emergency changes require upper management approval at Esri prior to release.

Once a change request is approved, the change is first applied to a staging environment. The staging environment may be launched temporarily for one-off changes or kept running 24/7 for engagements which require more frequent updates (monthly updates or more). Once Esri has applied changes in the staging environment, email verification by the customer will be required. Once the customer verifies staging, Esri will apply changes to production during the approved maintenance window. Once changes have been applied to production, email verification will be needed by the customer to close out the change ticket.

System Maintenance and Software Upgrades

Esri may need to perform regular system maintenance to the cloud environment, which may include tasks such as refreshing cloud server resources, clearing disk space, applying patches or system updates, etc. Esri will communicate a maintenance timeframe and expected downtime (if applicable) with customers as system maintenance is performed. Esri may request that the customer test the application to verify that it is available and working properly after maintenance is complete.

To upgrade Esri ArcGIS software with a service pack or later software version than what was originally deployed to production, Esri will need to coordinate with the customer to test the upgrade prior to updating the production environment. Once confirmed that the application has been tested and works in later versions of ArcGIS, Esri will coordinate the update through the standard Change Management process described above.

Incident Reporting and Technical Support

After an application has been deployed and approved in production, Esri and the customer will develop a process by which to report incidents associated with the availability and performance

of the cloud environment. Esri Managed Cloud Services will not troubleshoot issues associated with the functionality of custom applications or data (e.g. bug fixes or errors in data). Such issues will have to be reproduced and addressed by either the customer's technical resources or Esri Professional Services. If an update to the application is needed as a result of implementing a fix, it will need to go through the standard Change Management process described above.

Esri will supply an email alias to the customer which is monitored 24/7 to report issues related to the availability of their apps data or overall system performance. The customer will be responsible for identifying select internal resources with authorization to report issues to Esri. All issues reported by end users of the customer's data and applications will need to through the customer "helpdesk" staff and must be triaged prior to escalating to the Esri Managed Cloud Services team.

Once the issue is identified and confirmed that it is related to the Esri Managed Cloud Services environment, Esri will apply a fix or workaround and notify the customer when the problem has been resolved. A root cause analysis will then be conducted to determine what caused the issue, what was done to resolve it and what will be done to prevent it from happening again in the future.

Sample Service Level Agreement (SLA)

Below is a sample service level commitments offered by EMCS to support customer production environments.

Coverage

Twenty-four hours per day, seven days a week, Esri will provide customers with reasonably necessary telephone or written consultation, as requested by the customer, in connection with the availability of the production hosting environment. Up to five authorized users from within the customer organization will be able to report issues associated with their production applications.

Response Times

Pre-approved customer technical representative(s) may report a problem to the EMCS operations team by electronic mail to an alias which is monitored 24/7. Esri shall use reasonable efforts to meet Target Response Time and other obligations under this agreement. A "Problem" is defined as a condition identified as a result of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant. The below table summarizes the severity level definitions and associated target response time that Esri will attempt to meet to resolve the identified problem(s) upon written notification of an issue by the customer.

Definition and Severity Level Descriptions

Severity Level	Definition and Examples of Problem Events	Target Response Time	Target Resolution Time
Severity 1	• All Data Centers are down (applies to systems/applications hosted at multiple sites) • Single Data Center is down (for systems/applications that are hosted at a single site only) • A catastrophic production problem, production system, network, or application is down, hangs indefinitely, there is no work around	**1 hour**	**4 hours**
Severity 2	• The system or application has lost its redundancy and now is a single point of failure ("no availability", no redundancy) (i.e. 2 of 3 load balanced servers or applications are down and at least 1 remains up) • Severely degraded system or performance (it is working but slow, a significant impact to the application/system users) • A workaround exists	**1 hour**	**8 hours**
Severity 3	• The system has N+1 availability (redundancy) (i.e. 1 of 3 load balanced servers or applications are down and at least 2 remain up) • A system/application has intermittent issues and is failed over to the redundant component to eliminate any intermittent issues. (**Key Qualifier**: If the redundant component has issues it could be failed back over to the component with intermittent issues). • Action not severe enough to take down during business hours unless the system has redundancy • A production fix to an incident that can wait until next approved maintenance window or after business hours • Third party vendor issue that will require longer than 8 hours to resolve and is redundant (i.e. part needed for a redundant system)	**4 hours**	**2 days**
Severity 4	• The system has N+2 availability (redundancy) (i.e.1 of 4 load balanced servers or applications are down and at least 3 remain up) • Low impact performance issues that may require: testing, additional hardware/software (has redundancy) • Parts needed to be ordered (has redundancy)	**2 days**	**3 days**

Upon written notification, Esri will determine the level of severity that applies to the specific incident, based upon the table above.

Service Levels and Remedies – Availability

Upon mutual determination and satisfactory evidence that Esri failed to make the production environment available in accordance with the service level system availability percentage in any given month during the term of the contract, excluding scheduled maintenance, this failure shall be deemed a service level default ("Service Level Default"). Ordering Entity may obtain the non-exclusive remedies set forth below. For purposes of this Agreement "Available" means that Ordering Entity and associated end-users of data content are able to have external HTTP or HTTPS access to the applications and data content required by the customer through the Internet.

Service Level Description

Service Level (Monthly)	Service Level Credit (Percentage of Monthly Fees)
Less than 99.9% and greater than 99%	10%
Less than 99%	25%

The service level described does not apply to unavailability, suspension or termination of the application, data or any other performance issues: (i) that is due to factors outside of Esri's control, including any force majeure event or Internet access or related problems, (2) that result from any actions or inactions of the customer or any third party (3) that result from customer equipment, software, or other technology, (other than third party equipment within Esri's direct control, (4) arising from Esri's suspension or termination of the customer's right to the hosted applications and data content in accordance with this agreement.

Credits, if determined to be applicable, shall be applied against the next invoice. In the event a Service Level Default occurs after the customer has given notice of termination or due to non-appropriation of funds, or an Ordering Entity has made final payment to Esri for the Managed Services and no further invoices shall issue as a result, Esri shall refund to the Ordering Entity the amount of the appropriate Service Level Credit due for the period of default. An initial root cause analysis (RCA) report will be provided within 48 hours of remediation.

The service levels described above do not apply to development, staging and training environments. They only apply to systems running in production.

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

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

Yes, Esri is able to comply with this requirement. The Esri team is organized around established geographic territories and named accounts. This model ensures complete account coverage and provides users with an established contact for their organization. Esri maintains an up-to-date list of territory assignments for all staff.

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

Esri offers technical support to customers who are current on software maintenance, as well as a Premium Support option at an additional cost. With Esri Premium Support, an Ordering Entity can request the help of a support technician, either by phone or email, 24 hours a day, 7 days a week, 365 days a year.

Esri Managed Cloud Services

Esri Managed Cloud Services offers different levels of support depending upon the service level that the customer selects. Support is provided during business hours (6am-6pm Pacific Time) for lower level offerings and 24/7 for higher level offerings. Refer to Section 8.4.1 for response times and communication protocols.

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

Esri Software and SaaS Offerings

The following table describes our issue severity levels and our goals for resolving these issues. Although we strive to meet the goals stated in the table, resolution times are often dependent on factors beyond our control. Some of these factors include operating system limitations, user-designated workflows, security issues, integration with third-party applications that have not been provided by Esri, and customer availability.

Severity	Criteria	Response Time	Resolution Time
Critical	These defects cause a severe impact on business operations (for example, disabling a critical business process). In the case of a critical issue, no workaround is available.	6 business hours	Esri will make a reasonable effort to resolve the problem or provide a workaround while keeping the customer updated at least every business day until the case is closed.

Severity	Criteria	Response Time	Resolution Time
High	These defects cause a noncritical impact on business operations (for example, significantly degrading the quality or handling of data). In the case of a high-priority issue, no stable workaround is available.	8 business hours	Esri will make a reasonable effort to resolve the problem or provide a workaround while keeping the customer updated at least every business day until the case is closed.
Medium	These defects cause a minor impact on business operations.	2 business days	Esri will make a reasonable effort to resolve the problem or provide a workaround while keeping the customer updated at least every three business days until the case is closed.
Routine	These defects cause little or no impact on business operations.	2 business days	Esri will make a reasonable effort to resolve the problem or provide a workaround while keeping the customer updated at least every five business days until the case is closed.

Esri Managed Cloud Services

See section 8.4.1 for Esri Managed Cloud Services Service Levels and support models.

Yes, Esri is able to comply with this requirement. Esri's standard customer service has established response time standards.

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

Yes, Esri is able to comply with this requirement. Esri will offer a Value Added Service that supports Design.

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

Yes, Esri is able to comply with this requirement. We have Value Added Services that support this requirement.

Response to 8.5 (E) Security of Information

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Esri maintains a robust NIST 800-53 aligned set of information security policies and procedures which address the confidentiality of customer data and associated protection mechanisms. Esri's Cloud Hosting offerings provide options that are accredited for FISMA Low and FedRAMP Moderate sensitivity.

Data protection measures are based on the sensitivity of the information to be held. Prior to a cloud implementation / deployment, Esri will work with the Participating Entity to evaluate the Participating Entity's categorization of their data holdings and will then recommend an appropriate environment and data protection measures. Participating Entity's retain ownership of their data at all times.

Data disposal procedures use the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual"), or NIST 800-88 ("Guidelines for Media Sanitation") and other industry standard practices as applicable.

Managed Cloud Service Bundles (PaaS / SaaS)

Data protection controls for Esri's Managed Cloud Service bundles as provided by Esri Managed Cloud Services (EMCS) align with FedRAMP Moderate sensitivity. The confidentiality and integrity of customer data at rest is protected by implementing encryption of data sets (file servers and databases) using AES-256 FIPS 140-2 compliant encryption. Sensitive data is stored in secured locations within EMCS, encrypted in-transit and at-rest and monitored by a 24/7 Security Operations Center (SOC) for unauthorized access. This protects the confidentiality, integrity and availability of resident data. No use of a Participating Entity's data outside the boundary of the production environment is permitted for EMCS without permission from the Participating Entity. In rare cases, where sensitive data is provided to Esri physically, the data is handled according to the existing Media Protection Policy for federally regulated data.

If requested following completion of any contract services, the EMCS Security Administration team extract and/or dispose of data according to DoD 5220.00-M standard. The EMCS Security Administration team also performs standard DOD 5220.22-M wipes of EBS volumes which are not attached to any functioning system prior to deleting them

EMCS uses physical infrastructure provided by Amazon Cloud Services (AWS). When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed 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.

ArcGIS Online (SaaS)

Data protection controls align with FISMA Low sensitivity. ArcGIS Online provides administrators of a Participating Entity the option of requiring encryption in transit via HTTPS (TLS) for data transmitted to and from their ArcGIS Online organization.

With the ArcGIS Online offering, data management, including implementation of data backup and retention policies is the Participating Entity's responsibility. ArcGIS Online does not encrypt customer data at rest. However, Participating Entities can encrypt their data either through their application or by leveraging and enterprise cloud encryption gateway solution. Customers with data sensitivity concerns frequently choose to implement a hybrid solution where sensitive data is kept on premises or in a separate cloud with higher security measures, such as Esri's Cloud Hosting (EMCS) offering as described above.

At the conclusion of a contract, it is the Participating Entity's responsibility to extract any data or information from ArcGIS Online to a local machine, if desired, and to delete data from ArcGIS Online. ArcGIS Online uses physical infrastructure provided by Amazon Cloud Services (AWS) and Microsoft Azure. These Cloud Infrastructure providers use the techniques detailed in DoD 5220.22-M to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.

Self-Service Cloud Environments (IaaS)

With is offering, it would be the customer's responsibility to dispose any data and information at the conclusion of a contract based on organizational policies and procedures. Esri's Cloud GIS offerings utilize physical infrastructure provided by Amazon Web Services (AWS). AWS uses the techniques detailed in DoD 5220.22-M to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

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

Esri will comply with applicable laws, regulations, and standards related to data privacy and security in the provisioning its GIS Cloud offering.

Participating Entities are ultimately responsible for the categorization of their information assets. Esri will work with Participating Entities prior to entering into an agreement to understand their data categorization (High, Medium, or Low Risk as defined by FIPS 199). This will define the contractual, technical, and operational requirements for data privacy and security and the applicable contractual terms regulations governing the protection of that data. Esri has Cloud Hosting offerings that are accredited for FISMA Low and FedRAMP Moderate sensitivity.

Managed Cloud Service Bundles (PaaS)

EMCS compliance with data protection and privacy laws is aligned with the legal and regulatory framework set by FedRAMP and aligns with FedRAMP moderate requirements. Applicable standards frameworks include NIST and FIPS. Additional information about the FedRAMP standards, legal and regulatory framework is available here. https://www.fedramp.gov/about-us/governance/

ArcGIS Online (SaaS)

ArcGIS Online complies with data protection and privacy laws as they apply to provisioning of ArcGIS Online. ArcGIS online is compliant with FISMA low requirements and based on NIST SP 800-53 R3 controls. A mapping of these controls to ISO 27001 is available here. http://downloads.esri.com/resources/enterprisegis/FISMA_Low_ISO_Mapping.PDF. The ArcGIS Online privacy statement is certified compliant with independent, international industry accepted privacy statements including TRUSTe Certified Privacy Seal and EU Safe Harbor. Participating Entities retain ownership of their data and are responsible for compliance with laws and regulations specific to their industry or particular use of ArcGIS Online. ArcGIS Online uses cloud infrastructure providers that are compliant with ISO 27001 and FedRAMP moderate requirements.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments utilize physical infrastructure provided by Amazon Web Services (AWS) whose policies and procedures align with ISO 27001 and FedRAMP Moderate and other applicable data privacy and security standards. For more information on AWS compliance with privacy and security laws, see Amazon Web Services (https://aws.amazon.com/compliance/).

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Esri's cloud GIS offerings include physical, technical, operational, and management controls to set and enforce requirements that a Participating Entity's accounts and data are accessed only for legitimate business needs. Participating Entities retain ownership of their data at all times.

The Esri Employee handbook specifics acceptable terms of use of data and information assets for all Esri employees. Other Key controls for personnel managing ArcGIS Online or Managed Cloud Service bundles include Rules of Behavior (RoBs) that must be signed by all personnel

with administrative access to Esri Cloud GIS systems, limiting access based on defined need, separation of duties, monitoring and logging of account access, and appropriate disciplinary actions if violations occur.

Esri's Cloud GIS offerings including EMCS and ArcGIS Online utilize physical infrastructure from AWS and Microsoft Azure. These Cloud Infrastructure providers have implemented their own ISO 27001 and FedRAMP moderate compliant controls including security training employee access agreements, and limiting physical access to their data centers.

Managed Cloud Service Bundles (PaaS/SaaS)

Less than ten (10) Esri personnel have access to EMCS and privileges are assigned based on role and using the principle of least-privilege as mandated by FedRAMP Moderate requirements. EMCS administrators use two-factor authentication via smart cards. All Esri personnel accessing EMCS have been approved by EMCS ISSO and any personnel with permissions to read customer data are confirmed U.S. persons.

Prior to accessing EMCS, all employees must acknowledge and sign a Rules of Behavior (RoB) document that outlines technical and organizational responsibilities related to the access and use of EMCS. No use of a Participating Entities data outside the boundary of the production environment is permitted for EMCS without permission from the Participating Entity. EMCS RoBs restrict employees from accessing customer data or accounts for reasons other than legitimate business needs. Employees must abide by the terms of the RoB. The RoB is reviewed/updated/re-signed annually where employees are made aware of actions that might be taken in the event of a violation.

System events such as login/logout and item access are logged and audited based on FedRAMP moderate controls, and all accounts and associated privileges are reviewed annually at a minimum as part of compliance with FedRAMP Moderate requirements.

ArcGIS Online (SaaS)

Less than 10 Esri employees that are specialized ArcGIS online administrators have access to customer data and utilize X.509 certificates for authentication.

As part of ArcGIS Online FISMA Low accreditation applicable employees must sign a rules of behavior (RoB) document that includes specific terms of use for the handling of customer data in ArcGIS online.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Esri management of this offering consists of ensuring that the

environment is accessible and that all appropriate Esri software is available for management and configuration. Esri employees accessing this environment for administrative purposes undergo background screening as part of the hiring process and are subject to acceptable use polies and procedures for data and information as specified in the employee handbook. Participating Entities are responsible for the implementation of their own rules of behavior and access agreements that control how their users access accounts data.

The Self-Service Cloud Environments can use physical infrastructure from AWS. AWS has implemented ISO 27001 and FedRAMP moderate compliant controls including security training employee access agreements, and limiting physical access to their data centers.

For more information on their compliance information, see Amazon Web Services (https://aws.amazon.com/compliance/).

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

Response to 8.6 (E) Privacy and Security

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

Esri has significant experience providing guidance and implementing solutions that meet government and industry security standards. Esri is actively engaged with government and research groups in the establishment of security guidelines for cloud implementations that serve as the basis for developing government cloud security standards like FedRAMP.

Esri strives to continuously advance the capabilities of our products to meet customer demands, including capabilities that help us improve our alignment with the essential characterizes on cloud computing as defined by NIST 800-145.

- EMCS is a FedRAMP moderate compliant SaaS/PaaS offering
- ArcGIS Online is a FISMA low compliant SaaS offering

For additional compliance details for Esri's Cloud GIS offerings please see Trust.arcgis.com (http://doc.arcgis.com/en/trust/)

Esri Cloud GIS offerings currently utilize physical infrastructure from Microsoft Azure and Amazon. These cloud service providers are in compliance with various standards from NIST, ISO, and SAS that address both security and cloud computing. For additional details please see for Microsoft® Azure (https://azure.microsoft.com/en-us/support/trust-center/compliance/)

information and Amazon Web Services (https://aws.amazon.com/compliance/) for Amazon compliance information.

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Esri has significant experience providing guidance and implementing solutions that meet government and industry security standards. Esri is actively engaged with government and research groups in the establishment of security guidelines for cloud implementations that serve as the basis for developing government cloud security standards like FedRAMP.

Esri ensures compliance of information systems with the organizational security policies, and standards to include regularly checking systems against compliance with security implementation standards and regulatory requirements. Compliance is a joint effort of legal, human resources, and security teams. Esri is Safe-Harbor self-certified to ensure appropriate handling of our customers' private information. Esri has documented guidelines and procedures for the secure configuration of our products and applications.

The following industry security standards are used (additional details are available at trust.argis.com)

- NIST 800-53. Security controls implemented for Esri's Cloud GIS offerings align with NIST 800-53.
- FISMA LOW. ArcGIS Online has been granted FISMA LOW ATO by the USDA. Controls are aligned with NIST 800-53 R3.
- FedRAMP Moderate. Esri's Managed Cloud Services (EMCS) offering has been granted FedRAMP moderate ATO by the US Census Bureau. Controls are aligned with NIST 800-53 R4
- Esri utilizes the Common Vulnerability Scoring System (CVSS) to facilitate categorization of vulnerability risks.
- USGCB. ArcGIS Desktop versions 9.3, 9.3.1, and version 10 were FDCC self-certified. FDCC has been superseded and evolved into USGCB, therefore ArcGIS Desktop version 10.1 and higher are USGCB self-certified.

Esri's Cloud GIS offerings (including EMCS, ArcGIS Online, and Self-Service Cloud Environments) are based on cloud infrastructure currently provided by Amazon Web Services (AWS) and Microsoft Azure. These cloud infrastructure providers comply with a number of government and industry standards and hold various security certifications and accreditations. Esri's cloud infrastructure providers will continue to obtain the appropriate security certifications

and conduct audits to demonstrate the security of the physical infrastructure upon which Esri Cloud GIS offerings are based.

More detailed information regarding the security in place from Amazon can be found here: http://aws.amazon.com/security/For more information on their compliance information, see Microsoft® Azure (https://azure.microsoft.com/en-us/support/trust-center/compliance/) and Amazon Web Services (https://aws.amazon.com/compliance/).

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

Esri's practices to secure data and applications hosted in our cloud systems focus on minimizing the potential attack surface and on continually monitoring information systems to detect and mitigate potential vulnerabilities. Esri's Cloud GIS offerings include appropriate controls to segment customers that are co-located in the same data center.

Managed Cloud Service Bundles (PaaS/SaaS)

EMCS is designed and developed to be a hardened environment that limits exposed services and minimizes the potential attack surface. Robust firewall rules are implemented using Amazon security groups as part of existing network hardening procedures. EMCS uses AES-256 encryption and FIPS 140-2 compliant algorithms for both data in transit and at rest.

All customers (tenants) must access the EMCS application tier using HTTPs (over port 443) and pass through a Web Application Firewall (WAF). At the application tier, tenants have separate instantiations of GIS infrastructure. At the data tier, tenants can optionally share common GIS databases and file systems with logical segmentation, or utilize single tenant, dedicated infrastructure when higher security assurance is required. Data isolation processes align with FedRAMP Moderate requirements.

Virtual Local Area Networks (VLANs) are implemented for each server role restricting inbound/outbound access to the minimum required range of ports to support functional operation of the system. Infrastructure is further logically separated to isolate customer data flows from administrative data flows using Virtual Private Cloud (VPCs).

Vulnerability assessments occur monthly by EMCS Security Administrators and a full risk assessment including security control review, vulnerability assessment and penetration testing occur annually by a FedRAMP accredited third party assessment organization (3PAO).

Automated scanning and manual testing are performed against application and programming interfaces to align with industry standards such as OWASP. Endpoint protection and centralized configuration management software are used within EMCS to continuously monitor all systems to detect the presence of unauthorized software. Unauthorized software components are

quarantined and Security Administrators are notified. Any software to be added to any EMCS system must be authorized through existing change control procedures. Patches and security fixes are fully tested in a test environment prior to deployment on production systems. These are implemented in a timely manner to meet established FedRAMP timelines for flaw remediation. These are mandatory requirement as part of FedRAMP Continuous Monitoring and ensure potential threats are identified, tracked and mitigated to provide constant security assurance.

ArcGIS Online (SaaS)

ArcGIS Online Data protection controls align with FISMA Low sensitivity. ArcGIS Online provides a Participating Entity's administrator with the option of requiring encryption in transit via HTTPS (TLS) for data transmitted to and from their ArcGIS Online organization. ArcGIS Online does not encrypt customer data at rest. However, a Participating Entity may choose to encrypt their data either through their application or by leveraging and enterprise cloud encryption gateway solution. Customers with data sensitivity concerns frequently choose to implement a hybrid solution where sensitive data is kept on premises or in a separate cloud with higher security measures, such as Esri's EMCS offering as described above.

ArcGIS Online is a multitenant environment. For hosted feature services specifically, Participating Entities are provided with their own logically separated database providing isolation of stored features. In addition, each data record within multitenant storage is stamped with the ID of the owning subscription to ensure a Participating Entity's data is accessible only by that Participating Entity's users. Some customers choose to implement a hybrid solution to further segment more sensitive data.

ArcGIS Online releases which include patches and bug fixes are performed quarterly. If security vulnerabilities are found or reported, they are assessed by the ArcGIS Online Leads, and fixed. If the vulnerability is critical, a patch is released, otherwise the fix is put into the next quarterly release. ArcGIS Online vulnerability management aligns with FISMA Low requirements and includes continuous monitoring to ensure any issues are resolved within defined timelines commensurate to assessed risk level.

Self-Service Cloud Environments (IaaS)

Esri offers Self-Service Cloud Environments based on cloud infrastructure provided by AWS. Using this offering, it would be the Participating Entity's responsibility to secure its data and applications, for example by implementing encryption, identity and access management (IAM), network segmentation, or monitoring. Esri can work with participating entities to help design and implement the cloud hosted system to address their specific needs for application and data security.

For more information on securing data and applications in the Self-Service Cloud hosting offering, please see http://aws.amazon.com/security/

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

Esri's Cloud GIS offerings include standards and practices to maintain data confidentiality. Key controls include data encryption, Rules of Behavior (RoBs) that must be signed by all personnel with access, limiting access based on defined need, separation of duties, monitoring and logging of account access, and appropriate disciplinary actions if violations occur.

Physical infrastructure providers for Esri's Cloud GIS Offerings (AWS and Microsoft Azure) have implemented their own ISO 27001 and FedRAMP moderate controls in their data centers to maintain data confidentiality. These include restricting access by job function so that only essential personnel receive authorization to manage cloud infrastructure services. Physical access authorizations utilize multiple authentication and security processes: badge and smart card, biometric scanners on-premises security officers, continuous video surveillance. Data center access is monitored and audited.

Managed Cloud Service Bundles (PaaS/SaaS)

With this offering, Participating Entities are responsible for the categorization and classification of their owned data hosted within EMCS. Security controls aligning with FedRAMP Moderate ensure sensitive data is stored in secured locations within EMCS, encrypted in-transit and at-rest and monitored by a 24/7 Security Operations Center (SOC) for unauthorized access. This protects the confidentiality, integrity and availability of resident data.

Less than ten (10) Esri personnel have access to EMCS and privileges are assigned based on role (e.g. security, administration, database administration) and using the principle of least-privilege as mandated by FedRAMP Moderate requirements. Approval for accounts must be obtained from the ISSO. Any employee with access to EMCS will have credentials revoked if transferred, dismissed or leaving the organization based on existing revocation procedures.

Prior to accessing EMCS, all employees must acknowledge and sign a Rules of Behavior (RoB) document that outlines technical and organizational responsibilities related to the access and use of EMCS. EMCS RoBs restrict employees from accessing a Participating Entity's data or accounts for reasons other than legitimate business needs. The employees must abide by the terms of the RoB. The RoB is reviewed/updated/re-signed annually and employees are made aware of actions that might be taken in the event of a violation.

System events such as login/logout and item access are logged and monitored by a 24/7 Security Operations Center (SOC) and all accounts and associated privileges are reviewed annually at a minimum as part of compliance with FedRAMP Moderate requirements.

Handling of confidential data includes policies for devices and how EMCS is accessed. EMCS Administrators connect from whitelisted IP addresses and require 2-factor authentication. For internal infrastructure identification, EMCS uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards. Esri has a BYOD policy and mobile security and acceptable use is part of the security awareness training however EMCS staff do not use mobile devices for administering, accessing EMCS or for storing customer data.

ArcGIS Online (SaaS)

With ArcGIS Online, Participating Entities are responsible for the categorization and classification of their owned data hosted within EMCS. Data stored within ArcGIS Online meets FISMA Low categorized requirements. Esri maintains a robust NIST 800-53 aligned set of information security policies and procedures which address the confidentiality of customer data and associated protection mechanisms

Less than 10 Esri employees that are specialized ArcGIS online administrators have access to customer data and utilize X.509 certificates for authentication. As part of ArcGIS Online FISMA accreditation applicable employees must sign a rules of behavior document.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provides a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Esri management of this offering consists of ensuring that the environment is accessible and that all appropriate Esri software is available for management and configuration.

In this environment, customers are responsible for implementing their own solutions to appropriately maintain data confidentiality. This may include developing their own rules of behavior and access agreements that control how user accounts and data are accessed.

The Self-Service Cloud Environments can use physical infrastructure from AWS. AWS has implemented ISO 27001 and FedRAMP moderate compliant controls including security training employee access agreements, and limiting physical access to their data centers. For more information on their compliance information, see Amazon Web Services (https://aws.amazon.com/compliance/). AWS provides FIPS 140-2 compliant solutions for encryption.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

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

Esri Cloud GIS offering includes the following third party attestations and accreditations.

- ***FedRAMP Moderate.*** EMCS is a FedRAMP moderate agency-authorized offering under Managed Services. EMCS achieved FedRAMP Moderate Authority to Operate (ATO) from the US Census Bureau. As part of FedRAMP Moderate requirements, a FedRAMP accredited third party assessment organization (3PAO) performs an annual audit that includes a full review across the entire set of security controls, vulnerability assessments across web application, network, system and database as well as a penetration test.

- ***FISMA Low.*** ArcGIS Online has been granted FISMA Low ATO by the USDA. ArcGIS Online utilizes third-party auditors that periodically review security controls in alignment with FISMA Low compliance. Continuous monitoring of ArcGIS Online includes vulnerability assessments and security control reviews.

- ***ISO 27001 / 27002.*** Esri's Self-Service Cloud Environments (IaaS) offering can use AWS as the provider for physical infrastructure. AWS infrastructure controls comply with ISO 27001 / 27002. Please see http://aws.amazon.com/compliance for additional details.

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

Esri monitors its production Cloud GIS hosting environments (e.g. hardware, network, web services, databases GIS and non-GIS applications) for system health, to detect potentially malicious activity, and to track SLAs and usage of services and metrics for compliance and capacity planning. Events are logged and logs are analyzed by system administrators.

To maintain security certifications, security requirements are constantly being reviewed, improved, and implemented as part of a continuous monitoring program. Esri Cloud GIS systems are also periodically audited for compliance by 3rd party independent assessment organizations. The frequency of the audits is aligned with the requirements of a specific certification or accreditation.

Esri Cloud GIS offerings utilize cloud infrastructure providers from MS Azure and Amazon Web Services (AWS). Each of these providers regularly audit their operations and can provide audit results under their own NDAs. Esri's cloud infrastructure providers will continue to obtain the appropriate security certifications and conduct audits to demonstrate the security of our infrastructure and services.

Managed Cloud Service Bundles (PaaS/SaaS)

EMCS performs monitoring and logging in alignment with FedRAMP moderate requirements. Monitoring requirements are documented in the EMCS Continuous monitoring guide. EMCS is front-ended by a Web Application Firewall (WAF) and an Intrusion Detection System (IDS) is deployed. Malware-protection is deployed on all end points including but not limited to: workstations, laptops, servers, database servers and the mobile devices of EMCS personnel.

These components (in addition to log data) are monitored by a 24/7 Security Operations Center that performs real-time analysis to detect malicious activity. EMCS logs are fed into an enterprise Security Information and Event Management (SIEM) system to perform correlation of suspicious behavior based on both signature and heuristic analysis. Examples of some of the events that are logged are: successful login events, unsuccessful login events, account management, object access, policy change and privilege functions. The logs capture sufficient detail to conduct proper audit and investigative measures if suspicious activity has been noticed. All audit records are maintained for a minimum of ninety (90) days to align with FedRAMP Moderate requirements. The EMCS implementation ensures only EMCS Administrators can read logs. Collected logs may not be modified or deleted by anyone.

As part of the continuous monitoring process, and to maintain FedRAMP moderate accreditation, a full security control review and risk assessment is conducted annually which includes associated policies, procedures and standards as they relate to EMCS. This yearly review is conducted by an accredited third party assessment organization (3PAO).

The EMCS IaaS provider (AWS) undergoes the same assessment as part of maintaining their FedRAMP Moderate compliance.

ArcGIS Online (SaaS)

ArcGIS Online performs logging and auditing at the system level to align with FISMA Low requirements. This includes monitoring of key security parameters to identify potentially malicious activity on the systems. ArcGIS Online also logs user and usage statistics across all users and groups in an ArcGIS Online organization and provides administrators with tools to view these logs.

ArcGIS Online is audited by 3rd Party Auditors in accordance with FISMA Low requirements. Continuous monitoring includes vulnerability assessments and security control reviews.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, monitoring / auditing and scalability requirements are the responsibility of the user. Esri will monitor the environment to make sure it is accessible and that all appropriate Esri software is available for management and configuration.

The **Self-Service Cloud Environments** can be based on infrastructure currently provided by Amazon Web Services (AWS). AWS includes monitoring and auditing capabilities in alignment with ISO 27001 and FedRAMP. Additional information is available here https://aws.amazon.com/security/services/.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

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

Yes, Esri's Cloud GIS offerings provide the capability to define access privileges based on role and to restrict visibility to specific users and groups. Further, Esri's cloud GIS offerings let users configure access using Enterprise Logins and their SAML compliant identity providers (IdPs). In this way Participating Entities can leverage existing authentication mechanisms as well as existing organization-approved policies, procedures and processes for account provisioning and revocation. Cloud infrastructure providers ensure multifactor authentication is used for their administrative operations.

Managed Cloud Service Bundles (PaaS/SaaS)

EMCS supports integration with SAML 2.0 compliant Identity Providers (IdP) to ensure users can leverage existing authentication mechanisms as well as existing organization-approved policies, procedures and processes for account provisioning through revocation. This also includes the capability to configure an organization's multi-factor authentication solution to align with requirements such as HSPD-12, PIV, and CAC. EMCS access is whitelisted to applicable IP addresses. EMCS Administrators connect from whitelisted IP addresses and require 2-factor authentication.

Authorization is based on Role. Roles define what a specific user can see. Default roles are Administrator, Publisher, and User. It is also possible to configure custom roles if more granular security permissions are required.

ArcGIS Online (SaaS)

Customers can choose to use the built-in ArcGIS Online user store or use Enterprise Logins which allows customers to leverage their AD/LDAP by using a SAML 2.0 compliant identity provider (IdP). ArcGIS Online users can configure their Enterprise logins to utilize their organization's two-factor authentication solution which can align with requirements such as HSPD-12, PIV, and CAC. In addition, customers can also choose to enable multi-factor authentication for their organization independent of Enterprise Logins.

ArcGIS Online privileges are assigned based on Role. There are three default roles of Administrator, Publisher, and User. Customers can also create their own custom roles (https://doc.arcgis.com/en/arcgis-online/administer/configure-roles.htm) to more granularly define privileges. In addition, ArcGIS Online uses a 'group' based sharing model where items can be shared with specific groups of users in the customer's ArcGIS Online organization. Roles define the privileges of the user while groups define what they can see.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. With this offering, it is the Participating Entity's responsibility to manage identities and access to cloud hosted data and documents. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

The ArcGIS Platform as well as Amazon which can be the physical infrastructure provider of the Self-Service Cloud Environments incorporate solutions for identity and access management. The ArcGIS Platform provides the ability to restrict access to data at the application and service level. Please see Trust.arcgis.com (http://doc.arcgis.com/en/trust/) for additional information. For additional information on identity and access management capabilities of AWS https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

Managed Cloud Services Bundles include Security Incident Response Plans that align with the security accreditation of the specific Cloud GIS offering (FISMA Low for ArcGIS Online and FedRAMP Moderate for Managed Cloud Services Bundles).

Security Incident management follows the procedures documented in the Security Incident Response Plan. The plan defines roles and responsibilities, key capabilities, training, and

security incident handling process (preparation, detection and analysis, containment, eradication, and recovery, and post incident activities) that must be followed for security related incidents.

Security Incident notification procedures vary depending on the type and severity of a security incident. Esri's standard is to notify a customer of a security incident impacting the customer's data or information within 72 hours. This follows the standard established by DFARS 252.204-712.

Managed Cloud Service Bundles (PaaS/SaaS)

EMCS Incident Response policies, procedures and processes align with FedRAMP Moderate. EMCS has a specific communication plan depending on the nature of the incident to ensure proper legal precautions are taken and chain of custody is maintained throughout an incident.

As part of alignment with FedRAMP Moderate requirements, EMCS personnel are required to report suspected security incidents to the organizational incident response capability within timelines recommended by US-CERT specified in NIST SP 800-61 (as amended). Points of contact for law enforcement and other authorities are maintained. As detailed in the Incident Response Plan for EMCS, incident response communication and involvement beyond Esri and the EMCS ISSO may include: the Participating Entity, Amazon, Law enforcement, US-CERT, the FedRAMP PMO, and others as necessary.

ArcGIS Online (SaaS)

Security incident management is delineated within ArcGIS Online's Incident response plan documentation which aligns with FISMA LOW requirements. Information security incidents are classified into severity levels and processed according to severity level. In the case of a confirmed data breach that impacts the customers data, Esri notifies the customer within 72 hours per the standard established by DFARS 252.204-712. Esri will coordinate with appropriate parties to investigate the security breach and will take commercially reasonable steps for remediation based on Esri's assessment of risk. Esri will provide updates to the Participating Entity with applicable information on a mutually agreed upon schedule.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, and scalability requirements are the responsibility of the Participating Entity. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

Security incident handling procedures as they pertain to Esri's IaaS offering will be defined based on the specifics of an engagements with a Participating Entity.

Physical cloud infrastructure can be provided by Amazon Web Services (AWS) which includes its own incident response plans and procedures in alignment with ISO 27001.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

Esri Cloud GIS offerings including both Managed Cloud Service Bundles (EMCS) and ArcGIS Online are subject to data flow controls both in the form of subnets and VLANs. Specifically, each solution is subject to separation of Data Zone, Application Zone, DMZ Zone, and Security Zone. Furthermore, within EMCS, each customer environment is implemented on a separate virtual private cloud network that completely isolates its systems from other customer systems, (e.g. while it is possible for the core EMCS infrastructure to interact with all customer solutions for the purpose of scanning, policy alignment, configuration management, and auditing, no customer system can directly contact another customer system.)

For customers utilizing ***Esri's Self-Service Cloud Environments (IaaS)***, this offering can be based on infrastructure provided by Amazon Web Services (AWS). Participating entities can isolate servers in any number of ways, including restricting servers and data centers to specific Amazon regions.

AWS utilizes multiple separate network segments. Using Amazon Virtual Private Cloud (Amazon VPC) lets customers provision a private, isolated section of the Amazon Web Services (AWS) Cloud to launch AWS resources in a virtual network as defined by the customer. With Amazon VPC, customers can define a virtual network topology that closely resembles a traditional network they might operate in their own datacenter. Customers have complete control over their virtual networking environment, including selection of IP address range, creation of subnets, and configuration of route tables and network gateways.

Securing data at the application level remains entirely in the control of the Participating Entity.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

Esri's Cloud GIS offerings include Managed Cloud Services Bundles (PaaS), ArcGIS Online (SaaS) and Self-Service Cloud Environments (IaaS).

Managed Cloud Services Bundles (PaaS/SaaS)

The EMCS environment has been architected following FISMA, NIST, and CIS guidance for FedRAMP moderate geospatial Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) authorizations of our customer environments.

EMCS provides customers with secure Geographic Information System (GIS) Solutions in the cloud and includes Application Infrastructure, Security Infrastructure, and Cloud Infrastructure.

EMCS enables quickly sharing geospatial content. Participating Entities maintain complete control over their applications and the access to their services and maps. Underlying security, administrative functions are managed by Esri. EMCS leverages physical cloud infrastructure from Amazon Web Services (EMCS).

Application Infrastructure. EMCS includes ready-to-use instances of ArcGIS running in the cloud. Key capabilities include a range of client applications, web services and web service publishing, map and application creation for web and mobile APIs, Geodata Management, and ArcGIS Server Manager to administer the application infrastructure.

EMCS provides Participating Entities with a PaaS or SaaS implementation option. The PaaS Architecture layer includes ArcGIS Server and Portal Web Service Endpoints as the major applications. The SaaS Architecture Layer includes ArcGIS Server and Portal applications. Customers may optionally choose a clustered database infrastructure shared across customers, or have their own database infrastructure instances spun up on single-tenant hardware.

Security / Administrative Infrastructure. The EMCS security infrastructure provides system administration and security through a combination of tools and services. EMCS is front-ended by a Web Application Firewall (WAF) that aids in DDoS mitigation. Furthermore, an IDS is deployed throughout EMCS to work in conjunction with the WAF to detect signature-based and anomaly-based ingress/egress traffic for malicious activity. The EMCS security architecture allows Participating Entities to implement complex password policies and leverage their own SAML 2.0 Identity Providers for identity and access management (including multi-factor authentication). Administrative functions provided by EMCS administrators include application deployment, testing, vulnerability scanning, ongoing data management (data updates, backup, and archive), technical support, monitoring, and supporting 24/7 Security Operations Center. EMCS Test/staging and production environments are separated.

Cloud Infrastructure. For physical cloud infrastructure (facilities, Hypervisor, TCP/IP, hardware, network, storage), EMCS leverages the Amazon Web Services (AWS) East / West Regions FedRAMP moderate cloud infrastructure which also aligns with ISO 27001 standards. Refer to AWS virtual machine image link below. http://aws.amazon.com/ec2/vm-import for additional information.

ArcGIS Online (SaaS)

The ArcGIS Online security architecture has been implemented based on NIST 800-53 R3 security controls and is in compliance with FISMA Low requirements.

ArcGIS Online has been architected a secured, reliable geographic information system (GIS) delivered using the software-as-a-service (SaaS) model and provides as complete, cloud-based mapping platform. ArcGIS Online services are elastic, available on demand, managed by Esri, and can be accessed by Participating Entities running on a wide range of platforms. Access is subscription-based, and Participating Entities do not need to provision separate infrastructure to use ArcGIS Online services.

Capabilities. Through an ArcGIS Online subscription, Participating Entities have immediate access to a rich suite of tools and hosting capabilities, and applications to store, manage, and host mapping services. ArcGIS Online also allows users to easily publish geographic content within and beyond an organization. Major ArcGIS Online components include Content Management, Content Publishing, Work Anywhere, Executive Access, Public Access, Collaboration and Workflow Management, Catalog and Data Discover, Hosted Web Services, User-Generated Web Applications, ArcGIS Online Services

Security / Administration. As a SaaS offering, ArcGIS Online is fully managed by Esri. No end user action is required to manage administrative functions such as updates to software and services, performance, scalability, security or server configuration. The ArcGIS Online security architecture allows Participating Entities to implement complex password policies and leverage their own SAML 2.0 Identity Providers for identity and access management (including multi-factor authentication). ArcGIS Online is scanned on a regular basis to ensure application security meets industry standards such as OWASP. ArcGIS Online Test/staging and production environments are separated. ArcGIS Online uses Cloud Infrastructure provider firewalls and host based firewalls are utilized to separate various ArcGIS Online components.

Cloud Infrastructure. ArcGIS Online uses cloud infrastructure from Microsoft Azure and Amazon Web Services (AWS) which aligns with ISO 27001 and FedRAMP Moderate.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments are architected to simply provide a supported computing environment where Purchasing Entities have full control of all provisioning and monitoring for their cloud environments. Esri will ensure the environment is accessible and that all appropriate Esri software is available for the Participating Entities management and configuration. Physical cloud infrastructure can be provided by Amazon Web Services (AWS) and includes facilities, Hypervisor, TCP/IP, hardware, network, and storage.

Server configuration, performance, security, monitoring, and scalability requirements are the responsibility of the Participating Entity. With this offering it is the Participating Entities responsibility to deploy and run software (which may include operating systems or applications)

and manage access to the data and software services that are deployed. The participating entity in turn may leverage these offerings to in turn deliver technology to their users using a variety of service models (e.g. PaaS or SaaS).

Self-Service Cloud Environments can use cloud infrastructure from Amazon Web Services (AWS) which aligns with ISO 27001 and FedRAMP Moderate. The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Esri conducts new-employee background investigation/ screening for all new employees. The content of the Esri new-employee investigation is conducted using the TalentWise Hire™ service and includes: an employment verification check, and a criminal background check for any conviction of a violent crime or crime of theft, dishonesty or breach of trust. The background check shall be performed in any governmental construct (e.g., state, county, province, territory) throughout the world in which the Employee has resided during the seven (7) years preceding his/her employment with Esri. A positive result for that investigation is a requirement for employment at Esri. This investigation is conducted by the Esri Human Resources department.

Newly hired personnel sign an agreement covering adherence to established governance and security policies. All employees are required to attend security awareness training every two years.

Employees with access to customer data in Esri Cloud GIS systems undergo additional screening and training as applicable based on the sensitivity of the information to be handled.

Esri Cloud GIS environments utilize infrastructure from Amazon Web Services (AWS) have their own security training and employee agreements that align with ISO 27001 standards.

Managed Cloud Services Bundles (PaaS/SaaS)

Personnel screening and rescreening activities reflect applicable federal laws, executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions and are aligned with FedRAMP moderate requirements.

Employees requiring access to EMCS must fill out an additional access request form and sign a Rules of Behavior (RoB) document annually that outlines technical and organizational responsibilities. Esri employees working on EMCS (less than 10) obtain account privileges through existing account provisioning processes and approval must be obtained from the EMCS ISSO. Two-factor authentication using approved smartcards is required by EMCS administrators and access to the infrastructure is limited by segmentation and using a bastion host. Any

employee with access to EMCS will have credentials revoked if transferred, dismissed or leaving the organization based on existing revocation procedures.

There is specific security awareness training for employees that develop and maintain EMCS. Role-based training and annual refresher training is required and enforced through a series of tests. Security awareness training includes but is not limited to topics such as: insider threats, security responsibilities, advanced persistent threats, anti-phishing, mobile, social engineering awareness and cloud security. In addition to role-based training for employees accessing and administering EMCS, security awareness training and mandated refresher training is in place. This ensures compliance with FedRAMP Moderate requirements.

EMCS Administrators are segregated based on organizational and administrative roles and utilizing the principle of least privilege. Role-based access control is used to assign different privileges to support specific functions including, but not limited to, Security, Administration, and Database Administration.

Accounts are centrally managed within the EMCS infrastructure. Account access and account management (create, modify, delete, disable) requests are logged and tracked by a 24/7 Security Operations Center. All accounts and associated privileges are reviewed annually at a minimum as part of compliance with FedRAMP Moderate requirements.

ArcGIS Online (SaaS)

As part of ArcGIS Online FISMA accreditation, employees working with ArcGIS Online must also sign a rules of behavior document further enforcing requirement with respect to information security and acceptable use of systems. Privileged access is monitored. Access to information system utility and audit tools is restricted to authorized personnel within ArcGIS Online. Operations personnel revoke physical and logical access privileges as part of the termination process.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, and scalability requirements are the responsibility of the Participating Entity. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration. Esri Personnel assigned to administer this environment will undergo background screening upon hiring as described above. Participating Entities are responsible to implement any background checking for their employees and to log their access to sensitive data based on their own organizational policies.

The Self-Service Cloud Environments can use physical infrastructure from AWS. AWS has implemented ISO 27001 and FedRAMP moderate compliant controls including security training

employee access agreements, and limiting physical access to their data centers. For more information on their compliance information, see Amazon Web Services (https://aws.amazon.com/compliance/).

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

Esri's security measures and standards follow the controls as defined in NIST 800-53 and are implemented based on the sensitivity and confidentiality of the data that must be protected. Protections for confidential data include encryption, segregated data and information flows, encryption, intrusion detection systems and monitoring.

Managed Cloud Services Bundles (PaaS/SaaS)

EMCS is designed and developed to be a hardened environment that limits exposed services and minimizes potential attack surface. Robust firewall rules are implemented using Amazon security groups as part of existing network hardening procedures.

Participating Entities are responsible for the categorization and classification of their owned data hosted within EMCS. Security controls aligning with FedRAMP Moderate ensure sensitive data is stored in secured locations within EMCS. The confidentiality and integrity of customer data at rest is protected by implementing encryption of data sets (file servers and databases) using AES-256 FIPS 140-2 compliant encryption. EMCS only permits connections on port 443 to FIPS 140-2 compliant end-points. Participating Entities and EMCS Administrators must connect to EMCS infrastructure using TLS only. Administration and Infrastructure keys are managed through key management which aligns with FedRAMP Moderate security requirements. Esri employees with access to EMCS have encryption at-rest on both their issued workstations and mobile devices.

System and data access is monitored by a 24/7 Security Operations Center (SOC) for unauthorized access. This protects the confidentiality, integrity and availability of resident data.

ArcGIS Online (SaaS)

Participating Entities are ultimately responsible for all data that is transmitted to and stored in ArcGIS Online. ArcGIS Online provides a Participating Entity's administrator the option of requiring encryption in transit via HTTPS (TLS) for data transmitted to and from their ArcGIS Online organization. ArcGIS Online does not encrypt customer data at rest. However, a Participating Entity can encrypt their data either through their application or by leveraging an enterprise cloud encryption gateway solution.

For customers with sensitive data where confidentiality/integrity is paramount, ArcGIS Online can be used in a hybrid deployment. This would mean ArcGIS Online is used for some data and supplemented by a separate ArcGIS for Server (on premise or in a separate cloud) with more sensitive information. This server could be hosted in a cloud that offers higher reassurance and more advanced security capabilities such as the Managed Cloud Services X-Large bundle with FedRAMP (http://doc.arcgis.com/en/trust/security/esri-managed-cloud-services.htm) offering or on premises at the customer location using their own enterprise security capabilities and infrastructure.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, and scalability requirements are the responsibility of the Participating Entity. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

This offering can use physical infrastructure from AWS. AWS aligns with ISO 27001 and offers capabilities for customers to encrypt data in transit and at rest using FIPS 140-2 compliant algorithms.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

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

Please see Questions 8.3.1 and 8.6.8 for a description of Esri's security incident and data breach handling procedures. Esri's Cloud offerings are for Cloud GIS and do not include handling of e-commerce data.

Response to 8.7 (E) Migration and Redeployment Plan

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Esri Managed Cloud Services will work with the Purchasing Entity to develop a plan to de-provision resources once a project has reached the end of its term meanwhile maintaining the contracted SLA throughout the remainder of the life of the contract. Depending upon the level of sensitivity of the data content, Esri will use pre-defined procedures for data removal and decommissioning.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

Esri Managed Cloud Services will work with a Purchasing Entity to determine what content needs to be preserved and delivered to the Purchasing Entity upon completion of a contract. Regular backup and archival of the content can be implemented to ensure all necessary data content is captured and stored so that it can be provided to the Purchasing Entity upon request.

Response to 8.8 (E) Service or Data Recovery

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

a. Extended downtime.

b. Suffers an unrecoverable loss of data.

c. Offeror experiences a system failure.

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

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

Esri Cloud GIS offerings have been engineered as fault-tolerant, high-availability environments to prevent scenarios of extended downtime, system failures, or irrecoverable data loss. Esri has Contingency Plans for its Cloud GIS offerings to ensure systems can be recovered in a planned, orderly fashion in case of severe system failures.

Apart from engineering our Cloud GIS offerings as highly available, physical and environmental controls of Esri's cloud infrastructure providers (AWS and Microsoft Azure) are aligned with ISO 27001 / 27002 and include environmental controls to manage temperature, HVAC, fire detection / suppression, and power (e.g. uninterruptible 24*7 power supply – UPS).

Contingency Planning

Esri has contingency plans for its Cloud GIS offerings that document disaster recovery procedures. Contingency planning and disaster recovery procedures are in alignment with the

specific security accreditations of Esri's cloud GIS offerings. (FedRAMP moderate for EMCS and FISMA Low for ArcGIS Online). Esri tests contingency plans on a regular basis. The main purpose of the testing is to get key teams familiar with the processes, assess the amount of time it takes to resume operations, and identify areas of improvement.

Esri's cloud infrastructure providers, Amazon Web Services and Microsoft Azure, have business continuity policies and plans that are in alignment with ISO 27001 standards.

Contingency plans contains detailed processes for assessing the impact of a service disruption. The includes the identification of critical services, impacts of disruption, recovery procedures and established Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for the systems.

This plans use a three-phase approach (Activation / Notification, Reconstitution, and Recovery) to recover and reconstitute the Esri Cloud Systems in case of a system failure. The approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. A final stage, deactivation, is used to document the recovery effort, incorporate lessons learned, and ready resources for any future events.

Additionally, the contingency plan defines the roles and responsibilities (including succession) training of personnel assigned to disaster recovery operations and testing of the processes and procedures defined in the plan.

Managed Cloud Services Bundles (PaaS/SaaS) Service or Data Recovery Capabilities

EMCS is a fully redundant system configured in an active-active configuration across two (2) separate AWS availability zones (data centers). In the event a primary instance fails, the second instance will automatically take on the additional load. This is transparent to end users.

EMCS uses redundant, relational databases to manage the integrity of feature data sets uploaded by customers. Databases are configured with SQL Server 2012 Always on. The cloud infrastructure providers also align with FedRAMP Moderate baseline to ensure integrity is maintained at all levels for EMCS.

The entire EMCS is monitored in real-time to ensure maximum service and meet capacity requirements.

By running redundantly in a high-availability environment, EMCS provides for immediate disaster recovery, should one of data centers become unavailable.

In addition to that, EMCS has built in additional disaster recovery capabilities in a third AWS data center. Daily full AMI backups and incremental database backups are stored to an S3 bucket in this data center. Should the two primary data centers that host the production deployment become unavailable (a highly unlikely scenario), AMI and data backups stored in a third Amazon data center are restored to any remaining Amazon datacenters. Please see Section 8.8.2 for additional information on backups.

Esri maintains a contingency plan for EMCS that incorporates the following: roles and responsibilities of key personnel, notification and escalation procedures, recovery plans, recovery time objective (RTO) and recovery point objective (RPO) and a clearly defined communication process. RPO and RTO, as well as default periods for backups are configurable based on customer requirements.

ArcGIS Online (SaaS) Service or Data Recovery Capabilities

ArcGIS Online utilizes redundant cloud infrastructure to minimize outages and is architected to take advantage of utilizing services and data across multiple AWS availability zones (data centers). Esri backs up ArcGIS Online infrastructure data regularly. Customer data is replicated to redundant infrastructure. The ArcGIS Online SLA can be found here: www.esri.com/~/media/Files/Pdfs/legal/pdfs/g-632-agol-service-level.pdf. The ArcGIS Online Health Dashboard is available at doc.arcgis.com/en/trust/system-status and provides the latest information on service availability. Customers can subscribe to an RSS feed to be notified of interruptions to each individual service.

ArcGIS Online provides Purchasing Entities with the ability to delete their data. However, it is the Purchasing Entity's responsibility to manage data retention and backup to their own requirements to minimize data loss. The best practice for backing up data from ArcGIS Online is to save individual copies of the data to a local machine. The recommended procedure to do this is to navigate to the content to be backed up, then download (for files) or export (for hosted feature layers) the data to a suitable location on the local machine. Data can be exported in common formats including shapefile or CSV. It is recommended to periodically back up data from a hosted feature layer that is updated frequently. A KBA describing backing up customer data is available at: http://support.esri.com/en/knowledgebase/techarticles/detail/41166.

Self-Service Cloud Hosting (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, and

scalability requirements are the responsibility of the user. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

With this offering, it would be the Participating Entity's responsibility to engineer a system that minimizes data loss and mitigates the effects of system failures or extended downtime.

The Self-Service Hosting offering can be based on physical infrastructure from Amazon Web Services (AWS).

AWS provides infrastructure services that can be used to design applications with a RTO ranging from hours to a highly available, multi-region system that is designed for continuous availability, by providing high availability services such as load balancing (ELB), auto scaling and multi-zone RDS. Data centers are located in multiple regions and within those regions there are multiple availability zones. Each availability zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Common points of failures like generators and cooling equipment are not shared across Availability Zones.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

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

a. Method of data backups

Managed Cloud Services Bundles (PaaS/SaaS)

EMCS uses Amazon Simple Storage Services (S3) for storage for short-term storage (database, filesystem, Amazon Machine Image (AMI) backups). Amazon Glacier is used for long term storage and archiving. To align with FedRAMP Moderate requirements, data backups are retained for a minimum of six (6) months or as required by a specific customer. Backup and Recovery measures are tested annually at a minimum to ensure effectiveness.

Backups are stored in hot Amazon data center and are secured based on Physical controls that align with a FedRAMP moderate sensitivity level. Backups are encrypted using FIPS 140-2 compliant algorithms and specific to the customer. (I.e. individual backup files for each customer). Only authorized personnel are allowed to retrieve backups from the offsite (virtual) storage location, and uploading of these backups to the active instance.

Esri's standard backup schedule provides for daily incremental and weekly full database backups. Multiple copies of backups are stored in transaction logs for applications that require incremental backups. The most recent backup would be used to restore the system in the event of a data loss or corruption. Data can also be archived for historical or legal purposes. Retention duration and the size of the data backup will impact costs associated with this level of service.

Backup frequencies and retention periods can be configured to meet specific needs. For example, Imagery data may be more static than other information. Therefore normal backup frequency for imagery data would waste resources. Other data sources (e.g. financial records may require longer retention periods. Esri will work with Participating Entities to define the specific frequencies and retention periods based on their data requirements

ArcGIS Online (SaaS)

Esri backs up ArcGIS Online infrastructure data regularly. Customer data is replicated to redundant infrastructure.

ArcGIS Online provides customers with the ability to delete their data. However, it is the Participating Entity's responsibility to manage data retention and backup to their own requirements. The best practice for backing up data from ArcGIS Online is to save individual copies of the data to a local machine. Please see Section 8.8.1 – ArcGIS Online for additional information.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, and scalability requirements are the responsibility of the user. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

In this environment, it is the customer's responsibility to manage data retention and backup (e.g. frequency, type, and location) to their own requirements. A KBA describing backing up customer data is available at:
http://support.esri.com/en/knowledgebase/techarticles/detail/41166.

This offering can be currently based on Amazon Web Services (AWS). AWS is based on a shared responsibility model which means that customers have full control over application stacks, including the operation system, running under their account. Customers or those providing application services for customers on AWS, have full control over backup procedures (data or server images) data retention periods and disposition.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

b. Method of server image backups

Managed Cloud Services Bundles (PaaS/SaaS)

When deploying applications to EMCS, Esri will create an "image" or custom AMI of the application and data deployed to the hosting environment that is then stored in S3 and used to

recover the system in the event there is an issue with an instance. This allows Esri to quickly recover and restore the environment to its original state. In EMCS full backups of AMIs are performed daily.

ArcGIS Online

Esri backs up ArcGIS Online infrastructure data regularly. Customer data is replicated to redundant infrastructure.

ArcGIS Online provides Participating Entities with the ability to delete their data. However, it is a Participating Entity's responsibility to manage data retention and backup to their own requirements. The best practice for backing up data from ArcGIS Online is to save individual copies of the data to a local machine. Please see Section 8.8.1 – ArcGIS Online for additional information.

Self-Service Cloud Environments (IaaS)

Please see Section 8.8.2 – Self-Service Cloud Environments.

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

Managed Cloud Services Bundles (PaaS/SaaS)

Backups are stored in hot Amazon data center and are secured based on Physical controls that align with a FedRAMP moderate sensitivity level. Backups are encrypted using FIPS 140-2 compliant algorithms and specific to a customer. (i.e. individual backup files for each customer). Only authorized personnel are allowed to retrieve backups from the offsite (virtual) storage location, and uploading of these backups to the active instance.

No use of data from Participating Entity outside the boundary of the production environment is permitted for EMCS without permission from the Participating Entity. Participating Entities retain ownership of their data within EMCS. In rare cases, where sensitive data is provided to Esri physically (e.g. for tape backups), the data is handled according to the existing Media Protection Policy for federally regulated data.

Data backup and restoration procedures can be adjusted to meet a Participating Entity's requirements.

ArcGIS Online (SaaS)

Esri backs up ArcGIS Online infrastructure data regularly. Customer data is replicated to redundant infrastructure.

ArcGIS Online provides Participating Entities with the ability to delete their data. However, it is the Participating Entity's responsibility to manage data retention and backup to their own requirements. The best practice for backing up data from ArcGIS Online is to save individual

copies of the data to a local machine. For additional information, please see Section 8.8.1 – ArcGIS Online.

Self-Service Cloud Environments (IaaS)

Please see Section 8.8.2 – Self-Service Cloud Environments.

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

Managed Cloud Servcies Bundles (PaaS/SaaS)

EMCS is implemented utilizing AWS Cloud infrastructure. AWS provides a level of service that allows for application level continuity by providing 8 global regional locations including 4 in the United States, each with multiple datacenters.

EMCS has been implemented in Amazon Regions / data centers located in the United States. This applies to the primary data center, as well as alternates.

EMCS is fully redundant in an active-active configuration across two separate AWS availability zones (data centers) residing in different flood plains. This provides for immediate recovery should the primary instance fail.

In the unlikely event of two datacenters failing simultaneously, Amazon Machine Image (AMI) as well as database backups are saved to a third (hot) Amazon data center in a separate US region over 250 miles away and would provide for recovery from backups should the primary region become unreachable.

ArcGIS Online

ArcGIS Online is implemented in redundant Cloud infrastructure provided by AWS and Microsoft Azure. All data centers used are in the United States.

Self-Service Cloud Environments (IaaS)

Self-Service Cloud Environments can be based on infrastructure provided by Amazon Web Services (AWS). Participating entities can isolate data only to servers and data centers residing entirely in the United States of America by using US only regions and controlling access to that data. Securing data at the application level is entirely in the control of the Participating Entity.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

Response to 8.9 (E) Data Protection

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

Managed Cloud Services Bundles (PaaS/SaaS)

Data from Participating Entities is encrypted in transit and at rest. Administrators (EMCS or Participating Entity) must connect to EMCS infrastructure using TLS only. EMCS only permits connections on port 443 to FIPS 140-2 compliant end-points.

The confidentiality and integrity of Participating Entity's data at rest is protected by implementing encryption of data sets (file servers and databases) using AES-256 FIPS 140-2 compliant encryption. Esri employees with access to EMCS have encryption at-rest on both their issued workstations and mobile devices.

ArcGIS Online (SaaS)

Participating Entities are ultimately responsible for all data that is transmitted to and stored in ArcGIS Online. ArcGIS Online provides the Participating Entity administrator with the option of requiring encryption in transit via HTTPS (TLS) for data transmitted to and from their ArcGIS Online organization. ArcGIS Online does not encrypt customer data at rest. However, Participating Entities can encrypt their data either through their application or by leveraging an enterprise cloud encryption gateway solution.

For customers with sensitive data where confidentiality/integrity is paramount, ArcGIS Online can be used in a hybrid deployment. This would mean ArcGIS Online is used for some data and supplemented by a separate ArcGIS for Server (on premise or in a separate cloud) with more sensitive information. This server could be hosted in a cloud that offers higher reassurance and more advanced security capabilities such as the Esri Hosted Services / EMCS (http://doc.arcgis.com/en/trust/security/esri-managed-cloud-services.htm) offering or on premises at the customer location using their own enterprise security capabilities and infrastructure.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Participating Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments.

In this environment, it will be the Participating Entity's responsibility to implement encryption and other technology options to protect sensitive data. This offering can be deployed using

physical infrastructure from AWS which aligns with ISO 27001. AWS offers capabilities for customers to encrypt data in transit and at rest using FIPS 140-2 compliant algorithms.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Esri will comply with applicable laws, regulations, and standards related to data privacy and security in the provisioning its GIS Cloud offering.

Participating Entities are ultimately responsible for the categorization of their information assets. Esri will work with Participating Entities prior to entering into an agreement to understand their data categorization (High, Medium, or Low Risk as defined by FIPS 199). This will define the contractual, technical, and operational requirements for data privacy and security. Based on that, Esri will negotiate applicable contractual terms governing the protection of that data, including applicable Business Associate Agreements or any other agreement that may be necessary for data protection.

Esri has Cloud GIS offerings are accredited for FISMA Low (capable of storing and securing Low Risk data) and FedRAMP Moderate sensitivity (capable of storing and securing Moderate risk data.

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

With Esri's Cloud GIS offerings, customers retain ownership of their data at all times in accordance with the ownership provisions in the respective agreement.

In provisioning Cloud GIS services to a purchasing entity, Esri will not access a Purchasing Entity's accounts or use a Purchasing Entity's data for purposes other than as may be required to provide specific services under this Master Services agreement or terms of service agreed to as part of a participating addendum, SLA, or other contract document, or based on a purchasing entities written request. As such, access to a customer's account(s) or data is limited to legitimate business needs such as data center operations, trouble shooting, or responding to technical and service issues. Esri employees with access to Esri Cloud GIS systems sign rules of behavior documents (RoBs) that specify these restrictions and undergo training to understanding their obligations with respect to the handling of customer data.

Esri has implemented numerous physical, technical, operational, and management controls to set and enforce requirements that Esri employees with access to Esri Cloud GIS systems will access customer's accounts and data only for legitimate business needs. For additional details, please see Section 8.5.3.

Response to 8.10 (E) Service Level Agreements

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Please see a sample Service Level Agreement for Esri Managed Cloud Services in section 8.4.1. Esri is amenable to negotiating the Service Level agreement on a case by case basis. Price adjustments may be warranted should an Ordering Entity desire a non-standard response time.

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

Please see a sample Service Level Agreement for Esri Managed Cloud Services in section 8.4.1

Response to 8.11 (E) Data Disposal

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

Data disposal procedures use the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual"), or NIST 800-88 ("Guidelines for Media Sanitation") and other industry standard practices as applicable.

ArcGIS Online uses physical infrastructure provided by Amazon Cloud Services (AWS) and Microsoft Azure. These Cloud Infrastructure providers use the techniques detailed in DoD 5220.22-M to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.

Managed Cloud Services Bundles (PaaS/SaaS)

If requested following completion of any contract services, the EMCS Security Administration team extract and/or dispose of data according to DoD 5220.00-M standard. The EMCS Security Administration team also performs standard DOD 5220.22-M wipes of EBS volumes which are not attached to any functioning system prior to deleting them

ArcGIS Online (SaaS)

At the conclusion of a contract, it is the Purchasing Entity's responsibility to extract any data or information from ArcGIS Online to a local machine, if desired, and to delete data from ArcGIS Online. ArcGIS Online uses physical infrastructure provided by Amazon Cloud Services (AWS) and Microsoft Azure. These Cloud Infrastructure providers use the techniques detailed in DoD 5220.22-M to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Purchasing Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

In this environment it will be the Participating Entities responsibility to extract data at the conclusion of a contract and to implement appropriate data disposal policies and procedures in their self-service cloud environment.

Self-Service Cloud Environments can utilize physical infrastructure provided by Amazon Web Services (AWS) whose policies and procedures align with ISO 27001 and FedRAMP Moderate. AWS uses the techniques detailed in DoD 5220.22-M to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry standard practices.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

Response to 8.12 (E) Performance Measures and Reporting

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

The Managed Cloud Services X-Large bundle offers up to a 99.9% uptime commitment to its users. To ensure our ability to maintain this level of service, Esri has enterprise tools that are used to measure system availability, and monthly reports can be provided to a customer upon request.

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

The ArcGIS Online SLA is available at www.esri.com/~/media/Files/Pdfs/legal/pdfs/g-632-agol-service-level.pdf.

Esri Managed Cloud Services sample Service Level Agreements can be found in Section 8.2.1.

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

See section 8.2.1 for information regarding the support and communication process for Esri Managed Cloud Services for incident response and change management.

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

See section 8.2.1 for information regarding example remedies and consequences for not meeting target response and resolution times for Esri Managed Cloud Services.

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

Planned downtime associated with making low impact changes or for performing routine maintenance on production systems for customers using Esri Managed Cloud Services will be communicated 1-2 weeks in advance. Any downtime events will be coordinated with the customer. To minimize downtime or issues associated with making updates and performing maintenance on a system, Esri will test all changes in a "staging" environment prior to promoting changes to production. Image snapshots are taken every time a major change is made in a production system so that in the event that a server becomes corrupt or no longer available, Esri is able to launch new systems based on the latest image snapshot.

Esri will work with the customer to determine a maintenance window to ensure impact to end users is minimal.

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

See section 8.2.1 for information regarding example remedies and consequences for not meeting target response and resolution times for Esri Managed Cloud Services.

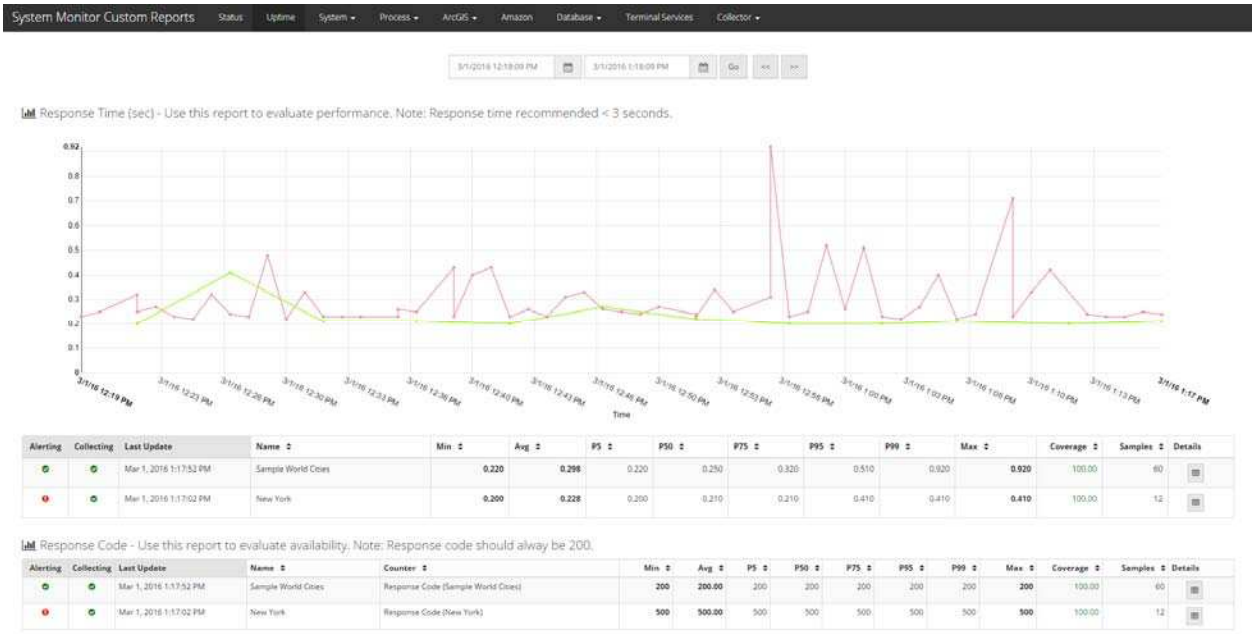
8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

Esri Software Products and SaaS Offerings

The latest information about ArcGIS Online service availability and performance is published through the ArcGIS Online Health Dashboard, available at doc.arcgis.com/en/trust/system-status.

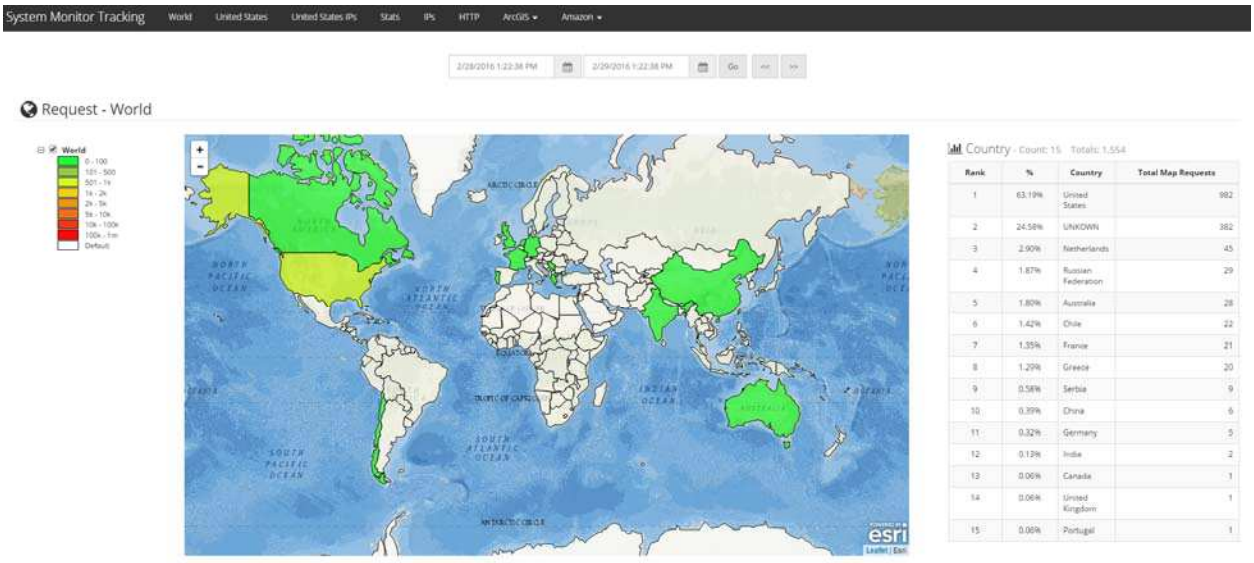
Esri Managed Cloud Services

Esri has developed custom reporting and monitoring tools tailored to support its products. Below is a screenshot of a sample report showing system uptime.



System Uptime

The screenshot below is an example report showing where requests are coming from globally and how many:



Example of Global Requests

Custom reports can be configured to meet the Purchasing Entity's needs.

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

Activity Dashboard for ArcGIS, available through the ArcGIS Online subscription status page, lets you track the way your organization uses ArcGIS Online. You can use Activity Dashboard for ArcGIS to view content summaries, user activity statistics, real-time reports, and other platform usage statistics. This lets you make more informed decisions about how to manage ArcGIS Online based on real-world user activity.

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

With Self-Service Cloud Environments the Participating Entity is responsible for provisioning new servers, as well as deploying and managing software. The Participating Entity may choose to setup remote access to their provisioned servers and is therefore free to deploy new data, services, and applications 24x365.

The Managed Cloud Services Bundles provide different support models for on-demand deployment. With the Small bundle Esri will provision the servers, but the Participating Entity is responsible for any new software deployments to their provisioned servers. The Participating Entity's representative is provided with an administrator account to the operating system to support this. With the other preconfigured bundles Esri manages the deployment of all software, and can support on-demand deployment 24x365.

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

The **Self-Service Cloud Environments** offering can be deployed on infrastructure provided by Amazon Web Services (AWS). In this offering the customer has direct access to the AWS Management Console, which can be used to scale up and scale down 24x365. New instances may be added in one hour or less. With these offerings it is the customer's responsibility to scale up and scale down. When provisioning GIS systems based on ArcGIS 10.1 for Server, the Participating Entity may also leverage the ArcGIS 10.1 for Server Cloud Builder software made available by Esri to facilitate both manual and automatic scaling of ArcGIS for Server software.

The Self-Service Cloud Environments may leverage other cloud providers to meet the particular requirements of the Participating Entity.

The **Managed Cloud Services Bundles** provide different support models for scaling up and down infrastructure.

With the Small bundle Esri manages the provisioning and de-provisioning of infrastructure. At the request of the customer, Esri can provision (i.e. scale-up) and de-provision (i.e. scale-down) infrastructure. The provisioning of infrastructure may require new task orders, and therefore may be subject to the terms and schedule of the NASPO contract administration process.

The Medium, Large, and X-Large include auto-scaling. The auto-scaling service allows for the dynamic scaling of server resources to address high demand on infrastructure resources. This

service not only allows the rapid deployment of new server resources but also removes servers when they are no longer needed, eliminating unnecessary costs associated with excess capacity.

Response to 8.13 (E) Cloud Security Alliance

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

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

Esri is providing CSA Level 1 responses (CCM) for ArcGIS Online and EMCS in Appendix B. Both questionnaires are also posted online on Esri's trust site – Trust.arcgis.com (http://doc.arcgis.com/en/trust/)

Esri's CSA answers for ArcGIS Online are in the CSA STAR registry. Responses for EMCS are scheduled to be added to the CSA Star registry.

As described in Section 8.1.3, Esri's offering also includes Self-Service Cloud Environments (IaaS). This offering can use Amazon Web Services (AWS) cloud infrastructure. The AWS CSA CAIQ questionnaire is published on the AWS compliance site at the following location:

https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

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

Esri is providing CSA Level 1 responses (CCM) for AGOL and EMCS in the form of CCM (See Appendix B). These questionnaires are also posted online on Esri's trust site – Trust.arcgis.com (http://doc.arcgis.com/en/trust/)

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

Not available.

d. Completion CSA STAR Continuous Monitoring.

Not Available.

Response to 8.14 (E) Service Provisioning

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

When asked to make an emergency change to a production system supported by Esri Managed Cloud Services, the request will need to be reviewed by the Change Advisory Board (CAB) to assess risk and review justification. Four members of the CAB have to review and approve a change before action can be taken.

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

The amount of lead time for provisioning Solutions depends upon what offering and level of service is going to be provisioned. For Self Service provisioning, once an account is set up, a user has the ability to provision compute resources immediately. For Esri Managed Cloud Services, lower level provisioning can occur within one week, whereas our more advanced offerings could take 3-4 weeks assuming all testing and verification of the Solution has been completed.

Response to 8.15 (E) Back Up and Disaster Plan

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

Managed Cloud Services Bundles (PaaS/SaaS)

Esri can support data backup and retention for long periods of time if this is defined as a legal requirement by a Purchasing Entity. The standard retention period for data aligns with FedRAMP moderate requirements and is 6 months. Retention periods are configurable based on a Purchasing Entity's requirements. Costs associated with data retention vary depending on the duration of the retention period and the process used to archive the data content.

ArcGIS Online (SaaS)

A Purchasing Entity's data is backed up to redundant infrastructure. In the ArcGIS Online environment, it is the Purchasing Entity's responsibility to manage data retention to their own requirements. A KBA describing backing up customer data is available at http://support.esri.com/en/knowledgebase/techarticles/detail/41166. The best practice for backing up data from ArcGIS Online is to save individual copies of the data to a local machine.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Purchasing Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments.

In this environment, it is the Purchasing Entity's responsibility to manage data retention and backup (e.g. frequency, type, and location) to their own requirements. A KBA describing backing up customer data is available at: http://support.esri.com/en/knowledgebase/techarticles/detail/41166.

This offering is currently based on Amazon Web Services (AWS). AWS is based on a shared responsibility model which means that Purchasing Entities have full control over application

stacks, including the operation system, running under their account. Purchasing Entities or those providing application services for Purchasing Entities on AWS, have full control over backup procedures (data or server images) data retention periods and disposition.

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

Esri has implemented a robust set of controls for disaster recovery address common cloud computing risks such as data loss, or failures of cloud infrastructure.

Esri's Cloud GIS Offerings include infrastructure from AWS and Microsoft Azure. These cloud infrastructure providers use geographically redundant data centers to mitigate the impact of wide areas disasters and other events. Cloud infrastructure provider controls align with ISO 27001.

These cloud infrastructure providers have also been implemented environmental controls to protect data centers (aligning with ISO 27002 best practices) including Temperature control, Heating Ventilation and Air Conditioning (HVAC), Fire Detection and suppression systems, and Power Management. Data Centers have dedicated 24*7 uninterruptible power supply (UPS) and emergency power support.

Managed Cloud Services Bundles (PaaS/SaaS)

EMCS Disaster Recovery procedures are based on NIST 800-53 rev. 4 and meet requirements for systems with a FedRAMP moderate sensitivity. All procedures are documented in the EMCS Contingency Plan. The EMCS Contingency Plan is tested on an annual basis.

EMCS includes 24x365 monitoring of the Participating Entity's cloud infrastructure, web applications, database(s), and web services and will follow Esri's standard operational support and escalation procedures to maintain 99.9% system availability. Esri follows ITILv2 Best Practices for service support and service delivery and will follow these best practices to address issues related to the components monitored through this service level.

EMCS has been engineered to meet 99.9% availability. EMCS is a fully redundant system configured in an active-active configuration across two (2) separate AWS availability zones. In the event a primary instance fails, the secondary instance will automatically take on the additional load. This is transparent to end users.

In the unlikely event of two datacenters failing simultaneously, Amazon Machine Image (AMI) as well as database backups are saved to a third (hot) Amazon data center. Daily full AMI backups and incremental database backups are stored to an S3 bucket in a separate hot data center Should both (redundant) data centers running the production environment become unavailable, AMI backups and data backups stored in a third data center are restored to any remaining Amazon data centers.

ArcGIS Online

ArcGIS Online disaster recovery procedures align with FISMA Low. ArcGIS Online is implemented in redundant cloud infrastructure to minimize outages. ArcGIS Online infrastructure data is backed up regularly, and customer data is replicated to redundant data centers.

The availability of ArcGIS Online services is monitored, and the ArcGIS Online Health Dashboard, available at doc.arcgis.com/en/trust/system-status, provides the latest information on service availability. Customers can subscribe to an RSS feed to be notified of interruptions to each individual service.

Self-Service Cloud Environments (IaaS)

Esri's Self-Service Cloud Environments provide a supported computing environment for Purchasing Entities with the ability to remain in full control of all provisioning and monitoring for their cloud environments. Server configuration, performance, security architecture, and scalability requirements are the responsibility of the user. Esri will ensure the environment is accessible and that all appropriate Esri software is available for management and configuration.

Self-Service Cloud Environments can be deployed on Amazon Web Services (AWS). AWS provides a level of service that allows for application level continuity by providing 8 global regional locations including 4 in the United States, each with multiple datacenters. The continuity of any one application, however, is a function of how that application is architected to take advantage of the infrastructure services provided by AWS.

AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues, including a pager system so that alarms are reliably communicated to operations personnel.

Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a conferencing system is used which supports communication and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration.

Post-mortems are convened after any significant operational issue, regardless of external impact, and Cause of Error (COE) documents are drafted such that the root cause is captured and that preventative actions are taken for the future.

Implementation of the preventative measures is tracked during weekly operations meetings. The AWS data centers are designed to anticipate and tolerate failure while maintaining service levels. Data centers are built in clusters in various regions. All datacenters are online and serving

customers; no data center is "cold." The Amazon Incident Management team employs industry-standard diagnosis procedures to drive resolution during business-impacting events. Staff operators provide 24x365 coverage to detect incidents and to manage the impact and resolution of problems

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

Managed Cloud Services Bundles (PaaS/SaaS)

EMCS is implemented utilizing AWS Cloud infrastructure. AWS provides a level of service that allows for application level continuity by providing 8 global regional locations including 4 in the United States, each with multiple datacenters. Regions / data centers utilized for EMCS all reside in the United States.

EMCS is fully redundant in an active-active configuration across two separate AWS availability zones (data centers) residing in different flood plains. This provides for immediate recovery should the primary instance fail.

In the unlikely event of two datacenters failing simultaneously, Amazon Machine Image (AMI) as well as database backups are saved to a third (hot) Amazon data center in a separate US region over 250 miles away and would provide for recovery from backups should the primary region become unreachable.

ArcGIS Online (SaaS)

ArcGIS Online cloud infrastructure providers have business continuity policies and plans that are in alignment with ISO 27001 standards. ArcGIS Online utilizes redundant cloud infrastructure to minimize outages.

Self-Service Cloud Environments (IaaS)

Self-Service Cloud Environments can be based on infrastructure provided by Amazon Web Services (AWS). AWS data centers are built in clusters in 8 global regions (including 4 in the United States). All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration so that, in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AWS provides the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk floodplains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply

(UPS) and on-site backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.

In order to support disaster recovery, Participating Entities assume the responsibility to architect their AWS environment through self-service provisioning to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures. Esri has consulting packages available to assist Participating Entities with the design of an architecture which can support disaster recovery and high availability.

Response to 8.16 (E) Solution Administration

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

ArcGIS Online provides role-based access controls that let you manage user identities, accounts, and permissions fully within ArcGIS. Each user has a unique set of credentials that they use to access ArcGIS maps and apps. You can control access to content by restricting it to specific users, roles, and groups. You can also integrate your existing federated enterprise logins using SAML 2.0.

Managed Cloud Services Bundles support integration with SAML 2.0 compliant Identity Providers (IdP) to ensure users can leverage existing authentication mechanisms as well as existing organization-approved policies, procedures and processes for account provisioning and account revocation. EMCS uses role based authorization to restrict what content users can access and see. Default roles are Administrator, Publisher, and User. It is also possible to configure custom roles if more granular security permissions are required.

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

A number of key security parameters are monitored to identify potentially malicious activity on the systems. ArcGIS Online releases which include patches and bug fixes are performed quarterly. If security vulnerabilities are reported or found during regular vulnerability scans they are assessed by the security staff. Any vulnerabilities assessed as critical or high are patched immediately outside of normal patching routines. Cloud infrastructure provider anti-virus controls align with ISO 27001 requirements.

In alignment with FedRAMP Moderate requirements, EMCS ensures malware-protection is deployed on all end points including but not limited to: workstations, laptops, servers, database servers and the mobile devices of EMCS personnel. Furthermore, EMCS infrastructure is monitored by an Intrusion Detection System (IDS) to continuously monitor for signature and anomaly based attacks. A 24/7 Security Operations Center is monitoring these inputs in real-time

and potential threat events are immediately communicated. EMCS ensures malware-protection is deployed on all end points including but not limited to: workstations, laptops, servers, database servers and the mobile devices of EMCS personnel. Furthermore, EMCS infrastructure is monitored by an Intrusion Detection System (IDS) to continuously monitor for signature and anomaly based attacks. A 24/7 Security Operations Center is monitoring these inputs in real-time and potential threat events are immediately communicated.

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

Esri Managed Cloud Services has the ability to migrate Purchasing Entity data, metadata and usage data to alternative Cloud Hosting providers and will work with the Purchasing Entity to define this process. Esri will require a review of the successor Cloud Hosting solution provider's environment and resources to ensure that the Purchasing Entity's data, metadata and usage data can be maintained in an equivalent way.

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

Esri Managed Cloud Services can comply with this requirement. Esri has the ability to administer our solution to different participating entities.

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

Upon negotiating a participating addendum, Esri will work with a participating entity to apply their defined administration policy for managing a solution.

Response to 8.17 (E) Hosting and Provisioning

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

Esri has pre-configured images of its COTS technology that are used to provision geospatial resources in cloud environments. The following link provides more details regarding Esri's cloud ready images http://server.arcgis.com/en/server/latest/cloud/amazon/what-is-arcgis-server-on-aws.htm

8.17.2 Provide tool sets at minimum for:

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

Esri Managed Cloud Services utilizes cloud environments which have consoles that allow for quick provisioning of cloud resources such as virtual servers and storage devices.

2. Creating and storing server images for future multiple deployments

Esri Managed Cloud Services uses tools made available by Cloud Service Providers such as AWS and Azure that allows for imaging and backup. Image creation allows for the ability to quickly launch server resources without having to re-create from scratch.

3. Securing additional storage space

Esri's cloud partners provide the ability to add and remove storage for geospatial implementations. We have created scripts which allow for automated snapshots of cloud storage devices to ensure data remains intact and up to date.

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

Esri uses several types of tools that allow for monitoring and reporting on the status of cloud resources. These tools can be configured and provided to authorized personnel to show the status of availability and usage of the Participating Entities' geospatial resources.

Response to 8.18 (E) Trial and Testing Periods (Pre- And Post-Purchase)

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

The amount of time to support testing of the Esri Managed Cloud Services depends upon the user's testing workflows. We have had customers commonly engage with us in a proof of concept, similar to what was described in the references identified in section 6.2 above. These typically will last around 3 months before the user is able to complete all of their testing scenarios. Testing and training periods can be extended if it is determined that more time is needed.

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

The Self-Service Cloud Environments can be based on Amazon Web Services (AWS), which supports the ability to provision infrastructure for user test/staging that is identical to production. Through these offerings, Participating Entity technical representatives will have direct access to the AWS Management Console and are responsible for provisioning the infrastructure themselves.

The Managed Cloud Services Bundles all support the ability to host a user test/staging environment that is identical to production.

The Small bundle does not include a separate test/staging environment in the per server cost; however, at the request of the customer, such an environment can be provisioned and monitored.

The Medium, Large, and X-Large provide a staging environment for every application deployed to and supported in a production environment. Staging will have the same setup as production, will reside in the same hosting environment, and will be used to verify that the application functions properly when deployed to this environment. It is assumed that staging will be used only for verification and not for quality assurance (QA) testing. An environment specifically for QA testing can also be supplied upon request.

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

Esri's Self-Service Cloud Environments offering provides users with help documentation provided via the Cloud Service Provider (e.g. Amazon Web Services, Microsoft Azure, etc.).

Response to 8.19 (E) Integration and Customization

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

You can integrate your ArcGIS apps with solutions and services you host on premises, as well as services hosted by other organizations. ArcGIS provides APIs that are built on open RESTful communication patterns, letting you create mashups that combine ArcGIS services with information and tools from a wide range of applications, systems, and sources. This allows you to build on the valuable resources and tools that are available on the web and within your own organization.

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

When engaging with Purchasing Entities, Esri Managed Cloud Services will conduct an interview with the Entity to review their requirements and develop a Solution that will best fit their needs. Esri Managed Cloud Services has different "pre-configured" bundles that can be offered (Small, Medium, Large, and X-Large), however if it is determined that a Purchasing Entity needs something that falls outside of the scope of these Service Levels, we can design a custom bundle to suit fit the needs of the organization.

Response to 8.20 (E) Marketing Plan

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

Esri has dedicated sales teams who work with contacts within NASPO Participating Entities. These sales teams support State and Local governments, Higher Education, Non-profits and other industries and sectors who are eligible to purchase through NASPO. Through their work, organizations are able to realize their location strategies. These sales teams will play a central role in driving awareness of Esri's participation in NASPO. Esri has had experience working with State offices such as Washington and Hawaii using the previous WSCA contract for Cloud Solutions. In order to offer this contract to NASPO entities, Esri plans to promote this contract using the following outreach activities:

- The Esri/NASPO contract website
- An Esri/NASPO brochure or flier that could be delivered to Esri's many State and Local Government customers.
- Direct promotion of the NASPO contract to the State CIO and GIS offices through national organizations such as NSGIC and NASCIO
- Marketing pieces in publications such as ArcNews, GovTech Magazine
- Direct engagement with our existing GIS/IT customers in all of our States
- Targeted state and local government marketing campaigns which integrate Esri's participation in NASPO

Response to 8.21 (E) Related Value-Added Services to Cloud Solutions

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

Esri's value added services are designed to help Purchasing Entities throughout their cloud migration journey. Purchasing Entities seeking advice on which cloud solution best suits their organizational needs as well as Purchasing Entities experienced with the cloud but seeking services to get more from their cloud investment will find a solution to match their needs. Esri's goal is to help organization help themselves, enabling them to confidently make cloud adoption decisions and maximize their cloud investment.

The value added services Esri provides are outlined below:

Advice Services

System Architecture and Design

Designed for Purchasing Entities building new or migrating existing GIS to the cloud, the System Architecture and Design offer will equip Purchasing Entities with the information required to stand up a cloud environment to support their needs. Whether considering Amazon AWS, Microsoft Azure, or IBM SoftLayer, an Esri consultant will lead on-site activities to validate requirements, lead discussions, and evaluate cloud design alternatives. The purpose of the engagement is to determine an appropriate cloud GIS architecture for the needs and business drivers identified during this activity. As a result of these activities Purchasing Entities will receive cloud configuration specifications in a Cloud System Architecture and Design Report.

Cloud Readiness and Roadmap

A Purchasing Entity may choose to add a Cloud Readiness and Roadmap package to their System Architecture and Design Exercise. Leveraging the findings and assessments of the System Architecture and Design will allow Esri to determine the recommended activities for a Purchasing Entity to pursue in order to meet their cloud migration goals. Esri will provide consulting services to develop a Cloud Readiness Assessment and Migration Roadmap. The Cloud Readiness Assessment will classify the Purchasing Entity's GIS workflows, services, data, and applications against cloud migration criteria. The Migration Roadmap will identify a recommended order of migration of workflows, services, apps, and data to the cloud. It will also include suggested milestones, deliverables and a schedule a Purchasing Entity could use in its cloud-GIS migration.

Cloud Capacity Planning

Need specifications for a new server? This service addresses the number of CPUs, disk storage, RAM requirements, network hardware and system requirements for Esri products. A three-page summary of recommendations is provided.

Enablement Services

ArcGIS for Server Jumpstart for the Cloud

With ArcGIS for Server deployed in the cloud, you harness the power of the cloud while maintaining full control over your environment. To get started on using ArcGIS for Server in the cloud, Esri recommends an ArcGIS for Server Jumpstart. This service provides on-site configuration support and technology transfer on topics to assist you with getting started with

ArcGIS for Server and the cloud. An experienced Esri consultant will go through the points of using ArcGIS for Server on the cloud along with best practices to provide a smooth transition to the cloud. This service is ideal for Purchasing Entities looking to use Amazon Web Services, Microsoft Azure, IBM SoftLayer, or a hybrid cloud/on-premises approach.

WebGIS Jumpstart

The WebGIS Jumpstart gives a Purchasing Entity an introduction to the capabilities of WebGIS and demonstrates how to leverage it as part of the ArcGIS platform. This service is ideal for organizations looking to embrace the WebGIS pattern. This is accomplished with assistance from an Esri consultant who will help Purchasing Entity resources configure their WebGIS using an ArcGIS Online or Portal for ArcGIS. They may also review how to populate a Purchasing Entity's account with organizational content, and help resources learn best practices on how to use, publish, and administer content and services with WebGIS.

Performance and Scalability Testing

Is your GIS system ready for the volume of users in productions? This services provides test plan development, system configuration validation, testing scripts, and test execution to measure precisely how workflows perform and how your cloud environment scales under load. Performance metrics such as response time, throughput, and resource utilization including CPU, memory, disk I/O, and network bandwidth are monitored and collected. A testing report is provided following the on-site visit.

Proof of Concept

Purchasing Entities looking to migrate to the cloud may not always feel confident in how a cloud-based environment will work for their organization. The Proof of Concept is designed to equip organizations with the experiences and information they need to confidently make a cloud migration decision and plan. Esri consultants will work with the Purchasing Entity resources to establish baselines for key performance metrics. The Proof of Concept will take place over three phases: Discovery, Experience, and Reporting. During the Discovery phase, an Esri consultant will work to establish will explain key cloud KPIs and establish baseline measurements for the Purchasing Entity. While in the Experience phase, the Purchasing Entity will have access to an ArcGIS system which Esri will set-up, configure, and deploy in the cloud. Throughout the Proof of Concept, Esri will help the Purchasing Entity continue to measure the key performance metrics. At the end, the Purchasing will receive a report of how the system performed against the KPIs and how those compared to the baseline measurements.

Migration Services

Map, data, or application migration services

A Purchasing Entity can get support from an Esri consultant to migrate physical or virtual ArcGIS for Server servers to a cloud-based environment. The Esri consultant will migrate the ArcGIS for Server license, initiate a cloud-based ArcGIS for Server instance, and validate the server is running as expected. The consultant can be utilized to load data into the new cloud environment, migrate services, or assist in the migration of an existing application. During the engagement, the Esri consultant will employ an "I do, we do, you do" approach, initially doing, then working side-by-side with Purchasing Entity resources, and concluding by ensuring that the Purchasing Entity's resources are able to perform on their own.

Maximize Cloud Use

Cloud-based GIS Health Check

As a result of the Cloud-based GIS Health Check, Purchasing Entities will understand how their GIS system compares to Esri best practices, where improvements can be made, and receive recommendations based on the findings. This consulting services engagement provides a review and assessment of the overall state of a customer's cloud GIS implementation based on key best practices using a standard set of tools. This is a proactive activity designed to provide early detection of potential issues through a review of system configuration, workflows, error logs, system administration, and operations.

Cloud GIS Performance Assessment

Unsure what is causing slow performance in your cloud environment? Are your cloud costs growing faster than expected? This service will investigate cloud GIS system performance, including bottleneck detection and service bloat. During this engagement, an Esri expert will collect performance metrics, identify problems with system configuration and architecture, and discuss components that impact performance. Tools and methodologies will be used to isolate and diagnose performance issues. A report with findings and recommendations is provided following the on-site visit.

Performance Tuning

Is a specific GIS operation experiencing slow performance? This service will focus on addressing the performance pain points already identified in the Cloud GIS Performance Assessment. Esri resources will examine operation workload, application configuration, and the operating environment. Tools and methodologies will be utilized to trace and measure the effects of parameter changes and optimization.

Response to 8.22 (E) Supporting Infrastructure

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

The type of infrastructure required to support varying deployment models depends upon the level of service required. When engaging with Esri Managed Cloud Services, the team will assess the Purchasing Entities requirements and determine (1) what environment will best suit their needs, (2) the amount of infrastructure required depending upon usage and availability requirements, (3) the level of support needed from Esri to manage the Purchasing Entity's enterprise GIS systems.

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

For all Esri Managed Cloud Services offerings, the installation of new infrastructure will be provisioned and managed by Esri. Fees for such infrastructure will be passed along to the Purchasing Entity as a non-recurring or recurring cost depending upon the type of infrastructure provisioned. Esri will coordinate and notify Purchasing Entities before provisioning any new infrastructure that would result in a change in monthly payments.

Response to 8.23 (E) Alignment of Cloud Computing Reference Architecture

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

Esri Cloud Hosting (EMCS) provides both SaaS and PaaS based cloud services. For SaaS, some customers choose to utilize the offering to consume our Commercial Off the Shelf (COTS) capabilities as provided through ArcGIS Server and Portal for ArcGIS Products to utilize geospatial applications we host for them end-to-end. For PaaS, some customers utilize the offering to consume geospatial platform services that might get utilized by applications hosted within other locations, such as ArcGIS Online or their own on-premises applications. There are many variations as to how customers may specifically utilize EMCS, and while a SaaS deployment allows Esri to assume most of the responsibilities for managing and controlling the solution, some customers prefer the flexibility inherent with building a solution with Esri's geospatial platform components/SDKs and ArcGIS REST API.

7.0 Confidential, Protected or Proprietary Information

6.2 Scope of Experience

1. **State of Montana ($142,000 per year)**

Over time, demand and needs for GIS services have increased across the State. The State Information Technology Services Division (SITSD), who managed the State's GIS services and content did not have the resources to meet the increased demand nor did they want to invest in building them up both in infrastructure (hardware/network) and people (invest in GIS knowledgeable IT staff). Their environment did not have the ability to scale during peak needs (e.g., oil spill or wildfire).

SITSD worked with Esri Managed Cloud Services to outsource the management of their GIS service catalog. Before fully investing in Esri Managed Cloud Services, SITSD coordinated with Esri to engage in a proof of concept (POC) to verify and analyze the performance in this new cloud environment. Due to the success of the POC, they made the decision to move forward with moving over 50 of their GIS services and several terabytes for 9 departmental agencies as a centralized service. The cloud production environment was setup to be highly available and there is approximately 20TB data being stored for the State with the ability to add more data over time. Since the deployment into Esri Managed Cloud Services, the State has been able to decommission the environment that they maintained in-house.

2. **U.S. Department of Agriculture – OCIO ($47,000 per year)**

The ArcGIS platform facilitated a pilot USDA Enterprise Geospatial Repository for 8 agency participation. Managed Cloud Services supports hosting, while Esri Professional Servies supports USDA with jumpstart services, support jumpstart, design and eventual tech transfer to NITC for on-premises hosting.

Portal was taken to production for agency use in Q3 2014. 100 users licensed portal with IP addresses recognized access for USDA employees. Esri Managed Services also has stood up an instance of ArcGIS Server and geo-event processor for agency use and making resources publically discoverable.

After creating a successful Portal pilot for multi-agency use (see related opp - USDA: Department Geospatial Portal Pilot for Agency Collaboration & Discovery), the GIO/GMO requires a multi-server production environment with expanded services, elasticity & platform stability. The focus is to both support an expanding list of USDA agencies as well as sharing services for public access/consumption.

3. Avangrid, Inc. ($466,000 per year)

Avangrid is an energy services and delivery company serving about 2.7 million customers throughout upstate New York and New England, in the United States. Esri developed the Avangrid outage viewer application using the ArcGIS for JavaScript API in order to better support a disparate group of devices and browsers that would be accessing the outage viewer. This application was deployed and hosted on the Amazon Web Services cloud platform. Esri's Managed Cloud Services established the environment which included high availability and elastic instances to accommodate unforeseen user load during severe outages. Additionally, Avangrid required notifications and reports which provided insight into the utilization of the public outage viewer; Esri configured notification scripts which provided e-mail notifications to Avangrid and Esri resources of the utilization of CPU and elastic instance launches. Reports were configured to provide metrics on the types of usage. Upon completion of the JavaScript public outage viewer, Esri's Managed Services tested the application in a testing instance and built the deployment for the production instance. The application was deployed on time and the hosted environment has met client and user expectations.

Since the application has been in production it has invoked the environment's auto-scaling several times during large events such as severe storms and hurricanes. During these events the system was able to sustain the high user load by automatically adding resources to minimize downtime and performance impact to end users. After the events, the environment scales back unused resources during steady-state operations. To view the application click on the following link: http://outagemap.nyseg.com/nyseg/

4. U.S. Department of Agriculture – Food Nutrition Services (FNS) ($63,000 per year)

The Supplemental Nutrition Assistance Program (SNAP), formerly known as "Food Stamps" helps 40 million people a month put food on their table. With help from the Esri Professional Services developers and Esri Managed Cloud Services, USDA was able to quickly build a rich Retailer Locator and make it available in the cloud. The SNAP Retailer Locator is a user-friendly web based application that provides easy access to the location of the nearest SNAP approved stores. Primarily designed to help SNAP recipients, the tool is also helpful for state eligibility workers, community organizations (such as food banks), and others offering assistance to SNAP recipients. Stores that accept SNAP benefits will also benefit from SNAP participants having ready access to finding a SNAP approved store in their neighborhood.

GIS developers created a custom web-based GIS web application running on top of a cloud hosted ArcGIS for Server platform. Esri Professional Services performs data transformation of the SNAP retail location data which is updated two times per month. Esri is hosting the locator using Esri Managed Cloud Services who updates the SNAP data twice a month in a highly available, scalable production environment. In the last several years there have been very few performance issues or unplanned outages, Esri has staff and tools that monitor the application and the ArcGIS cloud platform 24/7. All staff must follow Esri Change and Incident

Management procedures when handling production systems in order to remain in compliance with best practices.

SNAP Retailer Locator link:

http://www.fns.usda.gov/snap/retailerlocator

5. **U.S. Department of Agriculture – Forest Service ($91,000 per year)**

The US Forest Service (USFS) Geospatial Service and Technology Center (GSTC) uses the FSTopo web application to maintain, update, and host 1:24,000 primary base series maps for internal personnel. The application is hosted by Esri Managed Cloud Services, and the Esri Production Mapping team standardizes the processes for developing and maintaining the maps. Over the last five years, Esri has provided ongoing support through a series of task orders. For example, Esri helped GSTC develop a Production Mapping FSEdit maintenance application as well as a newly enhanced web application interface hosted in a collocated data center in Seattle, Washington.

FSTopo is database driven and enables on-the-fly generation and downloading of large-scale topographic maps. The Web-based user interface allows access to FSTopo anytime from any USFS computer where users can browse and select data, then produce the desired map.

The FSTopo application meets basemap requirements of the USFS, offers production mapping for standardized development and maintenance, is a simplified and enhanced web application interface, and allows replication in the cloud to support replicated updates to the FSTopo application.

The FSTopo system was built on service-oriented architecture using Esri commercial off-the-shelf software. ArcGIS for Server provides the GIS Web services and portal functionality, respectively. This system is fully managed by Esri Managed Cloud Services who hosts the application on Esri servers, monitors, updates and maintains the FSTopo application and Oracle database.

6.3 Financials

Esri maintains a current rating of 5A3 with Dun and Bradstreet (Duns# 06-313-4175).

CUSTOM SOFTWARE, TECHNICAL DATA, AND ASSISTANCE LICENSE ADDENDUM (E600 08/22/2014)

Esri, 380 New York St., Redlands, CA 92373-8100 USA • TEL 909-793-2853 • FAX 909-793-5953

ARTICLE 1—DEFINITIONS

All words, phrases, or terms defined in other parts of this Agreement shall have the same meaning in this Addendum. The following additional words, phrases, or terms shall have the following meaning:

i. "Commercial Off-the-Shelf Software" or "COTS Software" means all or any portion of Esri's proprietary software technology accessed or downloaded from an authorized Esri website or delivered on any media in any format, including backups, updates, service packs, patches, hot fixes, or permitted merged copies, available under license to the general public.
ii. "Custom Software" means all or any portion of the computer software code, components, dynamic link libraries (DLLs), and programs delivered on any media provided in source, object, or executable code format(s), inclusive of backups, updates, or merged copies permitted hereunder or subsequently supplied under any Task Order, exclusive of Commercial Off-the-Shelf Software, or COTS Software.
iii. "Deliverables" means Custom Software or Technical Data specified for delivery or use by Licensee under a firm fixed price Task Order.
iv. "Map Data" means any digital dataset(s) including geographic, vector data coordinates, raster, or associated tabular attributes supplied by either party for use in the performance of any Task Order, which must be separately licensed from the vendor.
v. "Services" means consulting support that is being performed by Esri on a time and materials (T&M) hourly basis in exchange for compensation from Licensee.
vi. "Services Output" means any tangible output produced as a result of the Services provided by Esri under this Addendum. Services Output can include, but is not limited to, reports, training materials, and Custom Software.
vii. "Task Order" means an ordering document (purchase order, task order, or other authorizing document) generated by either Licensee or Esri for professional services issued under this Addendum and containing substantially the same information as outlined in the sample task order form attached as Attachment A. Any additional terms and conditions in Licensee's ordering or authorizing document will be void and may only be incorporated into this Agreement by written amendment signed by both parties.
viii. "Technical Data" means, without limitation, all technical materials including formula, compilations, software code or programs, methods, techniques, know-how, technical assistance, processes, algorithms, designs, data dictionaries and models, schematics, user documentation, training documentation, specifications, drawings, flowcharts, briefings, test or quality control procedures, or other similar information supplied or disclosed by Esri under any Task Order. Technical Data does not include COTS Software, COTS data, or COTS documentation, which must be separately licensed by Licensee under Esri's commercial Software license, or Map Data.

ARTICLE 2—TASK ORDERS AND PROJECT SCHEDULE

Esri shall provide Deliverables and/or Services as specified in a specific Task Order relating to the COTS Software identified in the Task Order.

Unless otherwise provided by Esri in writing, Esri's Contracts Manager for the Professional Services Division is authorized to agree to Task Orders. Licensee shall provide advanced written notification of the name and title of the representative authorized to sign Task Orders and bind Licensee. Each party may enter into Task Orders at its sole discretion and shall not have any obligation under a Task Order until it is signed by both parties.

Each party shall identify in writing the project manager who is responsible for the Services or Deliverables specified in Task Orders. By written notice, either party may replace the project manager at any time with a similarly qualified person.

The period of performance of each Task Order shall be specified in each Task Order.

ARTICLE 3—RESERVATION OF OWNERSHIP AND GRANT OF LICENSE

Except as specifically granted in this Article 3, Esri or its licensors own and retain all right, title, and interest in the Deliverables and Services Output. This Addendum does not transfer ownership rights of any description in the Deliverables or Services Output to Licensee or any third party. Subject to the terms and conditions set forth in this Addendum and effective upon the transfer, by any means, of the Deliverables or Services Output to the Licensee, Esri hereby grants to Licensee a nonexclusive, worldwide license in the Deliverables or Services Output to use, modify, and reproduce the Deliverables or Services Output in connection with Licensee's authorized use of COTS Software. The license grant in the immediately preceding sentence does not apply to Map Data, which Licensee must separately and directly license from the vendor.

Licensee shall retain any patent, copyright, or trademark or proprietary notices on all items licensed under this Addendum and shall take other necessary steps to protect Esri's or its licensor's intellectual property rights.

ARTICLE 4—PATENTS AND INVENTIONS

During the performance of Task Orders, the parties anticipate that inventions, innovations, and improvements ("Inventions") relating to the subject matter of such Task Orders may be conceived solely or jointly by principals, employees, consultants, or independent contractors (hereinafter called "Inventors") of the parties hereto.

The parties agree that, as of the effective date of this Agreement, Esri or its licensors own all intellectual property rights in the COTS Software. During the term of this Agreement, Licensee shall promptly notify Esri if Licensee becomes aware of any known or suspected infringement or violation of these rights.

Each party shall retain title to any Inventions made or conceived solely by its Inventors during the term of this Addendum, including, but not limited to, such Inventions that Esri's Inventors solely make or conceive while providing technical assistance pursuant to this Addendum. The parties shall jointly own any Inventions made or conceived jointly by Inventors from both parties.

Where only one party has title to an Invention, that party, at its sole discretion, shall have the right, but not the obligation, at its expense to (i) decide on whether or not to seek or maintain, or to continue to seek or maintain, patent protection in any country on such Invention; (ii) decide the extent and scope of such protection; and (iii) protect and enforce in any country any patents issued on such Invention.

Except as provided in the next paragraph, where an Invention is jointly owned, each party shall share equally the costs of acquiring protection for the Invention and furnish the other joint owner with assistance reasonably required for acquiring protection.

The acquisition or maintenance of protection shall not be abandoned by a joint owner (the "Assigning Owner") without giving the other joint owner (the "Beneficial Owner") an opportunity to intervene and acquire or maintain protection at the Beneficial Owner's expense. The Assigning Owner electing not to acquire or maintain protection on any Inventions in any country or countries shall assign such of its rights in such Inventions to the Beneficial Owner as is necessary to enable the Beneficial Owner to protect such Inventions in such country or countries at its expense and for its exclusive benefit. In such event, the Assigning Owner shall make available to the Beneficial Owner the Assigning Owner's Inventors and shall otherwise cooperate with the Beneficial Owner in order to assist the Beneficial Owner in protecting such Inventions. The Beneficial Owner shall reimburse the Assigning Owner for all reasonable out-of-pocket expenses incurred in rendering such assistance. If any such Inventions are so protected by the Beneficial Owner, then the Assigning Owner shall have a license with respect to the subject matter of such protected Inventions in such country or countries.

All Inventions made by Inventors during performance of tasks and activities defined by Task Orders during the term of this Addendum will be presumed, absent clear and convincing evidence to the contrary, to have resulted from the Inventors' activities under the Task Orders.

Neither party may license, transfer, sell, or otherwise alienate or encumber its interest in jointly owned Inventions without the written consent of the other party, which shall not be unreasonably withheld by either party. However, either party may transfer such Inventions to its Affiliates for their internal use only. "Affiliate" shall mean the parent or subsidiary companies

of a party or subsidiary companies to a party's parent provided there is more than fifty percent (50%) ownership of the subsidiary by the parent or party.

ARTICLE 5—CONFIDENTIALITY OF DELIVERABLES AND SERVICES OUTPUT

RESERVED

ARTICLE 6—ACCEPTANCE

A. For Time and Materials Task Orders. Services are provided strictly on a time and materials basis subject to the task order not-to-exceed funding limit. The Services delivered will be deemed accepted and in compliance with the professional and technical standards of the software industry unless Esri is notified otherwise by Licensee within ten (10) days after delivery.

B. For Firm Fixed Price Task Orders. Deliverables for fixed price Task Orders shall be categorized as follows:

i. "DELIVERABLE ACCEPTED" means a Deliverable conforming to applicable Task Order(s) with no more than minor nonconformities. Licensee shall complete its acceptance review within ten (10) working days of receiving each Deliverable.
ii. "DELIVERABLE ACCEPTED WITH REWORK" means a deliverable substantially conforming to applicable Task Order(s), but having a significant number of identified nonconformities and accepted subject to rework by Esri. Esri shall rework the Deliverable for the identified nonconformities and resubmit it within thirty (30) days. Licensee will rerun its acceptance review for the nonconformities detected in the initial review within ten (10) working days of such resubmission and will reclassify the deliverable as either DELIVERABLE ACCEPTED or DELIVERABLE REJECTED.
iii. "DELIVERABLE REJECTED" means a Deliverable that fails to substantially conform to applicable Task Order(s). Esri shall rework the Deliverable and resubmit it to Licensee within thirty (30) days, at which time Licensee shall have ten (10) working days to rerun its acceptance review and reclassify the deliverable as either DELIVERABLE ACCEPTED or DELIVERABLE REJECTED.

Licensee agrees it shall not use any Deliverable in its business operations before acceptance as described in B.i. or B.ii. If Esri does not receive within ten (10) working days after delivery written notice that the Deliverable is "ACCEPTED WITH REWORK" or "REJECTED" in accordance with B.ii. or B.iii., or if Licensee uses the Deliverable in its business operations, the Deliverable shall be deemed, as of the first to occur of either of these events, to have been accepted.

ARTICLE 7—CHANGES TO SCOPE OF WORK

Licensee may, at any time, request changes within the general scope of an open Task Order. If the parties agree to such changes and such changes cause an increase or decrease in the cost or time required to provide a Deliverable under any Task Order (regardless of whether the Deliverable itself is changed), an equitable adjustment in the price or schedule, or both, shall be made, and the Task Order shall be modified accordingly in writing and signed by both parties.

ARTICLE 8—COMPENSATION; INVOICES

A. For Time and Materials Task Orders. Esri shall prepare and submit to Licensee written monthly invoices showing the compensation due for work performed, including travel time, under Task Orders to the Licensee address listed on the Task Order. The amount invoiced will be equal to the number of hours expended during the previous month multiplied by the rates for labor categories set forth in Attachment B. Meals will be invoiced on a "per diem" basis in accordance with the full daily limits stated in the most current Federal Travel Regulations,.

Esri may reallocate the budget between activities, labor categories, and ODCs as necessary to facilitate the work effort, provided the overall price is not exceeded. In the event Esri reaches the funded not-to-exceed Task Order value and the activities are not completed, Licensee may increase the order funding to allow additional work to be performed, or Esri may stop work without further obligation or liability.

B. For Firm Fixed Price Task Orders. Unless otherwise specified in a Task Order, Esri shall prepare and submit monthly invoices based on the percent complete for each Deliverable as of the end of the preceding month. Upon acceptance of all Deliverables under a Task Order, the unpaid balance of the total Task Order value is due.

C. Payment. Licensee shall pay each invoice no later than thirty (30) days after receipt thereof. Payment shall be made to the Esri address identified on original Esri invoices.

ARTICLE 9—LIMITED WARRANTY AND DISCLAIMER OF WARRANTIES

RESERVED

ARTICLE 10—LIMITATION OF LIABILITY

RESERVED

ARTICLE 11—EXPORT CONTROL REGULATIONS

Licensee must comply with all applicable laws and regulations of the United States including, without limitation, its export control laws. Licensee expressly acknowledges and agrees that Licensee shall not export, reexport, transfer, or release COTS Software, Services Output, or Deliverables in whole or in part, to (i) any US embargoed country (including to a resident of any US embargoed country); (ii) any person on the US Treasury Department's List of Specially Designated Nationals; (iii) any person or entity on the US Commerce Department's Lists of Parties of Concern; or (iv) any person or entity where such export, reexport, or provision violates any US export control laws or regulations including, but not limited to, the terms of any export license or licensing provision and any amendments and supplemental additions to US export laws as they may occur from time to time.

ARTICLE 12 OBLIGATIONS UPON TERMINATION BY CONTRACTOR:

In the event of Termination by Contractor as allowed under the Master Agreement, Attachment A, Article 7, the following shall apply:

i. Upon termination by Contractor, all outstanding Participating Addendums shall be subject to cancellation, acceptance, or rejection, at the sole discretion of Contractor
ii. In the event of termination by Contractor, the due dates of all invoices for amounts owed by all Entities to Contractor shall be accelerated automatically so that such amounts become due and payable on the effective date of the termination, regardless of the payment term provisions set forth in this Addendum.
iii. Upon termination of this Agreement, , the parties shall have no further obligations pursuant to its terms, except that Articles 1(Definitions) , 4(Patents and Inventions), 5(Confidentiality) , 8 (Compensation, Invoices) , Limited Warranties and Disclaimers (Article 31 of the Master Agreement., , Limitation of Liability Article 14 (Taxes) , and Article 19 Assignment and Delegation shall survive termination. Unless Licensee has materially breached its obligations under this Agreement, Articles 3 (Reservation of Ownership) , 9(Limited Warranty). shall also survive termination. Except where specifically stated otherwise, any current or future cause of action or claim of one party because of any breach or default of the other party and any accrued license rights shall survive to the degree necessary to permit the complete fulfillment or discharge of the cause of action.

ARTICLE 13—RESTRICTIONS ON SOLICITATION

RESERVED

ARTICLE 14—TAXES

Values specified in Task Orders are exclusive of state, local, and other taxes or charges (including, without limitation, custom duties, tariffs, and value-added taxes, but excluding income taxes payable by Esri). In the event such taxes or charges become applicable to Deliverables or Services Output, Licensee shall pay any such taxes upon receipt of written notice that they are due.

ARTICLE 15—INDEPENDENT CONTRACTOR

Esri is, and at all times will be, an independent contractor. Nothing in this Addendum shall be deemed to create an employer/employee, principal/agent, or joint venture relationship. Neither party has the authority to enter into any contracts on behalf of the other party or otherwise act on behalf of the other party.

ARTICLE 16—FORCE MAJEURE

If the performance of this Addendum, or any obligation except the making of payments, is prevented, restricted, or interfered with by reason of fire, flood, earthquake, explosion, or other casualty or accident; strikes or labor disputes; inability to procure or obtain delivery of parts, supplies, or power; war, terrorist act, cyberattack, or other violence; any law, order, proclamation, regulation, ordinance, demand, or requirement of any governmental agency; or any act or condition whatsoever beyond the reasonable control of the affected party, the party so affected, upon giving prompt notice to the other party, shall be excused from such performance to the extent of such prevention, restriction, or interference.

ARTICLE 17 CLAIMS

RESERVED

ARTICLE 18—NOTICE

All notice required by this Addendum shall be in writing to the parties at the following respective addresses, or to such other address as a party may subsequently specify in a notice provided in the manner described in this Article, and shall be deemed to have been received (i) upon delivery in person; (ii) upon the passage of three (3) days following post by first class registered or certified mail, return receipt requested, with postage prepaid; (iii) upon the passage of two (2) days following post by overnight receipted courier service; or (iv) upon transmittal by confirmed e-mail or facsimile, provided that if sent by e-mail or facsimile, a copy of such notice shall be concurrently sent by US certified mail, return receipt requested and postage prepaid, with an indication that the original was sent by e-mail or facsimile and the date of its transmittal:

Licensee: _____
_____
_____
Attn.: _____
Tel.: _____
Fax: _____

Esri: Environmental Systems Research Institute, Inc.
380 New York Street
Redlands, CA 92373-8100
USA
Project/Technical Notice—Attn.: _____,
Senior Contract Administrator
Tel.: 909-793-2853, extension _____
Fax: 909-307-3034
Legal Notice—Attn.: Contract Manager
Tel.: 909-793-2853, extension _____
Fax: 909-307-3020
With a copy to _____, Contract Administrator

Notice for non-US Licensees shall be deemed to have been received (i) upon delivery in person; (ii) upon the passage of seven (7) days following post by international courier service with shipment tracking provisions; or (iii) upon transmittal by confirmed e-mail or facsimile, provided that if sent by e-mail or facsimile, a copy of such notice shall be concurrently sent by receipted international courier service, with an indication that the original was sent by e-mail or facsimile and the date of its transmittal.

ARTICLE 19—ASSIGNMENT AND DELEGATION

RESERVED

ATTACHMENT A
SAMPLE TASK ORDER
Esri Agreement No. _____
Task Order No. _____

In accordance with the terms and conditions of the above-referenced Addendum between Environmental Systems Research Institute, Inc. (Esri), and _____ (Licensee), _____ (Licensee Address), this Task Order authorizes preparation and provision of the Services Output and/or Deliverables described and in accordance with the terms, schedule, and start/end date(s) specified below.

1. Scope of Work: [As applicable, specifically identify and describe Services Output or Deliverables including Custom Code, Map Data, and Technical Data (including Technical Assistance) and the resources to be provided by Licensee (including Licensee-supplied personnel, software, hardware, and digital or hard-copy data), and place of delivery and location where technical assistance will be provided.]

   In addition to the foregoing, Licensee agrees that its employees, representatives, and subcontractors will cooperate and communicate with Esri during performance of this Task Order. Without cost to Esri, Licensee shall provide, allow access to, or assist Esri in obtaining all data Esri requests for performance of this Task Order, including, but not limited to, (1) copies of previously prepared reports, maps, plans, surveys, records, and other documents in the control or possession of Licensee and (2) copies of ordinances, codes, regulations, or other governmental documents.

2. Contract Type [Firm Fixed Price (FFP) or Time and Materials (T&M)]:

3. Total Task Order Value (if FFP) or Not-to-Exceed Value (if T&M):

4. Licensee Address for the Receipt of Esri Invoices:

5. Delivery Schedule or Start/End Date(s) for Each Deliverable:

6. Special Considerations:

7. Esri Project Manager: (insert name, telephone, fax, and e-mail address)
   Esri Senior Contract Administrator: (insert name, telephone, fax, and e-mail address)
   Licensee Project Manager: (insert name, telephone, fax, and e-mail address)
   Licensee Senior Contract Administrator: (insert name, telephone, fax, and e-mail address)
   Licensee Accounts Payable Contact: (insert name, telephone, fax, and e-mail address)

ACCEPTED AND AGREED:

_____	ENVIRONMENTAL SYSTEMS RESEARCH INSTITUTE, INC.
(Licensee)	(Esri)
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

ATTACHMENT B
TIME AND MATERIALS RATE SCHEDULE

PROVIDED SEPARATELY

IMPLEMENTATION SERVICES ADDENDUM FOR SERVICES PACKAGES

Esri, 380 New York St., Redlands, CA 92373-8100 USA • TEL 909-793-2853 • FAX 909-793-5953

1. DEFINITIONS

"Commercial Off-the-Shelf Software" or **"COTS Software"** means all or any portion of Esri's proprietary software technology accessed or downloaded from an authorized Esri website or delivered on any media, in any format, including backups, updates, service packs, patches, hot fixes, or permitted merged copies, available under license to the general public.

"Map Data" means any digital dataset(s) including geographic, vector data, coordinates, raster, or associated tabular attributes supplied by either party for use in the performance of this Addendum.

"Services" means consulting support being performed by Esri on a time and materials basis in exchange for compensation from Customer.

"Services Output" means any work product produced by Esri as a result of Services provided under this Addendum. Services Output can include, but is not limited to, reports, training materials, and custom software code.

"Services Package(s)" means a predefined unit of Services provided at a firm fixed price, as stated in Esri's proposal.

2. OWNERSHIP AND GRANT OF LICENSE

Except as specifically granted in this Addendum, Esri owns and retains all rights, title, and interest in Services Output. Subject to the terms and conditions in this Addendum, Esri grants to Customer a nonexclusive, royalty-free, worldwide license to use, modify, and/or reproduce Services Output in connection with Customer's authorized use of Esri's COTS Software.

3. PATENTS AND INVENTIONS

Esri and Customer will retain title to any inventions, innovations, and improvements ("Inventions") made or conceived solely by its principals, employees, consultants, or independent contractors ("Inventors") during the term of this Addendum. Esri and Customer will jointly own any Inventions made or conceived jointly by Inventors from both parties. Where Inventions are jointly owned, each joint owner will share equally the costs of acquiring protection for the Inventions and furnish the other joint owner with assistance reasonably required for acquiring protection. Neither Esri nor Customer may license, transfer, or sell its interest in jointly owned Inventions without the written consent of the other party, which will not be unreasonably withheld.

4. COMPENSATION

Esri will perform and invoice Services on a firm fixed price basis, and the deliverable will be consultation time. Esri will invoice Customer for all Services Packages ordered upon receipt of a valid Customer Purchase Order/ordering document. The Purchase Order/ordering document will confirm the quantity and price of the Services Packages ordered, as described in Esri's proposal or quotation, and will reference Customer acceptance of this terms and conditions document. Esri standard payment terms are net 30 days from receipt of an Esri invoice. Payment will be made to the Esri address identified on the Esri invoice. For Services provided beyond the period of performance proposed or provided in a new calendar year, Esri reserves the right to increase the Services Package price in accordance with Esri's most current price schedule. Esri's obligation for completion of the Services proposed is limited to the hours outlined in the Services Package descriptions within Esri's statement of work. If additional time is required to complete Customer's goals or activities set forth in the applicable statement of work, Esri and Customer will amend the Purchase Order/ordering document, as mutually agreed, by increasing the quantity of Service Packages ordered and issuing a new or amended Purchase Order/ordering document. Esri may, at its sole discretion, stop work to avoid exceeding the total hours allotted in a specific Services Package. Unused labor hours or travel remaining after the performance of a Services Package will expire and not be available for performance at a later date. If funded Services Packages have not been performed within twelve (12) months of the Esri invoice date, the Services Package will expire, and no refund will be provided. Any amendment to the Purchase Order/ordering document to add Services Packages will not affect the rights or obligations of the parties under this Addendum.

5. LIMITED WARRANTY AND DISCLAIMER OF WARRANTIES

Esri warrants for a period of ninety (90) days from the date of performance that Services will substantially conform to the professional and technical standards of the software industry. If Services do not substantially conform to these standards, Customer may require Esri to reperform Services at no additional cost to Customer. Services Output is provided as is without warranty of any kind.

Disclaimer of Warranties. With the exception of the limited warranty set forth in this Article, Esri disclaims and this Addendum expressly excludes all other warranties, express or implied, oral or written, including, without limitation, any and all warranties of merchantability or fitness for a particular purpose.

In addition to and without limiting the preceding paragraph, Esri does not warrant in any way Map Data. Map Data may not be free of nonconformities, defects, errors, or omissions; be available without interruption; be corrected if errors are discovered; or meet Customer's needs or expectations. Customer should not rely on any Map Data unless Customer has verified Map Data against actual data from documents of record, field measurement, or observation.

6. LIMITATION OF LIABILITY AND EXCLUSIVE REMEDY

RESERVED

7. CONFIDENTIALITY

RESERVED

8. EXPORT CONTROLS

Customer must comply with all applicable laws and regulations of the United States including, without limitation, its export control laws. Customer expressly acknowledges and agrees not to export, reexport, transfer, or release Services Output, in whole or in part, to (i) any US embargoed country (including to a resident of any US embargoed country); (ii) any person on the US Treasury Department's list of Specially Designated Nationals; (iii) any person or entity on the US Commerce Department's Lists of Parties of Concern; or (iv) any person or entity where such export, reexport, or provision violates any US export control laws or regulations including, but not limited to, the terms of any export license or licensing provision and any amendments and supplemental additions to US export laws.

9. GENERAL PROVISIONS

RESERVED