



Contract # AR2473

STATE OF UTAH COOPERATIVE CONTRACT

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

CDW Government LLC

Name

230 N. Milwaukee Ave.

Address

Vernon Hills

IL

60061

City

State

Zip

LEGAL STATUS OF CONTRACTOR

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

Contact Person Jumana Dihu Phone # 312.547.2495 Email jumdihu@cdwg.com
Vendor # 11462IB Commodity Code # 920-05

2. GENERAL PURPOSE OF CONTRACT: Contractor is permitted to provide the Cloud Solutions and related value added services 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: 9/27/2017 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: Appendix A to the Microsoft NASPO ValuePoint Enterprise Agreement for Government Partners ("GPEA")
- Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.**
8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
- All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
 - Utah State Procurement Code and the Procurement Rules.
9. Each signatory below represents that he or she has the requisite authority to enter into this contract.

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

CONTRACTOR

9/26/2017

Contractor's signature

Date

Tara K. Barbieri

Director, Capture

Type or Print Name and Title

STATE

Director, Division of Purchasing

9/27/17

Date

Solomon Kingston

801-538-3228

801-538-3882

skingston@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 Addendum¹ ("PA");
- (2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits² to the Master Agreement;
- (3) The Solicitation;
- (4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State;
- (5) Appendix A to the Microsoft NASPO ValuePoint Enterprise Agreement for Government Partners ("GPEA") and
- (6) 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 is non-public information that is designated confidential or that a reasonable person should understand to be confidential including (1) Customer Data (2) any Purchasing Entity's records, (3) personnel records, and (4) information concerning individuals. Confidential Information does not include information that (a) becomes publicly available without a breach of this agreement, (b) was lawfully known or received by the receiving party and specifically designated as non-confidential by the sender including all Customer Data, or (c) is a comment or suggestion one party volunteers about the other's business, products or services.

Contractor means the person or entity providing solutions under the terms and

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

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

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.

Customer Data means all data, including all text, sound, software, or image files that are provided to Microsoft by, or on behalf of, an Enrolled Affiliate through its use of the Online Services. All references to “Data” in the Master Agreement shall be deemed to mean Customer Data.

Data Breach See *defined term for Security Incident*.

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) shall have the same meaning as the term "protected health information" in 45 CFR CFR § 160.103 of HIPAA.

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 any unlawful access, use, theft or destruction to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in use, theft, loss, disclosure, alteration or destruction of Customer Data. All references to "Data Breach" in the Master Agreement shall be deemed to mean Security Incident.

Service Level Agreement (SLA) means the document which specifies the standards to which Microsoft agrees to adhere and by which it measures the level of service for an Online Service. Microsoft's current and archived prior version SLAs are available at the Microsoft Volume Licensing Site (www.microsoft.com/contracts or a successor site). With respect to any Microsoft Online Service ordered under the Maser Agreement, the most current SLA available at the onset of a subscription License term shall apply to

that Online Service for the duration of that subscription License Term, after which (for any subsequent renewal subscription License term) it will be superseded by the version current at the time of renewal.

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 sixty (60) days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon thirty (30) days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership,

Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate if default cannot be reasonably cured as allowed per Defaults and Remedies (section 10).

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. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any of Contractor's Employees who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing

Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

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

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

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

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

10. Defaults and Remedies

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

- (1) Nonperformance of contractual requirements; or
- (2) A material breach of any term or condition of this Master Agreement; or
- (3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or
- (4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against either party to this Master Agreement or to a Participating State or Purchasing Entity, or the appointment of a receiver or similar officer for any such party or any of such party's property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or
- (5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, the party claiming default shall issue a written notice of default, identifying the nature of the default, and providing a period of

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

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

- (1) Exercise any remedy provided by law; and
- (2) Terminate this Master Agreement and any related Contracts or portions thereof; and
- (3) In the event of default by the Contractor, and to the extent permitted by the law of the Participating State or Purchasing Entity, the Lead State shall have the right to suspend Contractor from being able to respond to future bid solicitations; and
- (4) Suspend Contractor's performance; and
- (5) Withhold payment until the default is remedied.

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

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. Subject to the exceptions below and the NASPO ValuePoint Participants' (as defined

below) compliance with the notice and defense provisions below, in the event of any defect or deficiency in any Contractor Products or Services purchased by a Participating Entity or Purchasing Entity, Contractor agrees to defend, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees (collectively, the "NASPO Value Point Participants") against third party claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to tangible property suffered by such third party and caused by the negligence, or willful misconduct of Contractor, its employees or subcontractors or volunteers, at any tier, during the performance of this Master Agreement (a "PI Claim"). This clause shall not be construed to bar any legal remedies Contractor may have with respect to the NASPO Participants' failure to fulfill their obligations pursuant to the Master Agreement or any Participating Addendum.

To qualify for such defense, the Participating Entities/Purchasing Entities shall promptly notify Contractor of any PI Claim of which the Participating Entities/Purchasing Entities become aware which may give rise to a right of defense pursuant to this Section. Notice of any PI Claim that is a legal proceeding, by suit or otherwise, must be provided to Contractor within sixty (60) days of the Participating Entities'/Purchasing Entities' first learning of such proceeding. If the Participating Entity's/Purchasing Entity's laws require approval of a third party to defend Participating Entity/Purchasing Entity, Participating Entity/Purchasing Entity will seek such approval and if approval is not received, Contractor is not required to defend that Participating Entity/Purchasing Entity. If a PI Claim is settled, to the extent permitted by law, the Participating Entities/Purchasing Entities shall not publicize the settlement and will cooperate with Contractor so that Contractor can make every effort to ensure the settlement agreement contains a non-disclosure provision.

Notwithstanding anything to the contrary contained herein, Participating Entities/Purchasing Entities agree that Contractor has no obligation for any PI Claim covered by this Section arising out of or resulting from the Participating Entities'/Purchasing Entities' or any of their respective employees', contractors' or agents' acts of negligence, gross negligence or misconduct. THE FOREGOING SHALL CONSTITUTE EACH AND EVERY PARTICIPATING ENTITY'S/PURCHASING ENTITY'S SOLE REMEDY AND CONTRACTOR'S SOLE AND EXCLUSIVE LIABILITY FOR ALL PI CLAIMS.

b. Indemnification – Intellectual Property. Subject to the NASPO Participant's compliance with the notice and defense requirements and exceptions set forth below, Contractor agrees to defend the NASPO Participants against any claims made by an unaffiliated third party that any Product or Service or its proper or reasonably expected or acceptable use infringes that third party's patent, copyright, or trademark or makes unlawful use of its trade secret (an "Intellectual Property Claim").

(1) The Contractor's obligations under this section shall not extend to any claims based on:

- (a) Contractor's compliance with a Participating Entity's/Purchasing Entity's designs, specifications or instructions; or
- (b) Contractor's use of technical information or technology provided by the Participating Entity/Purchasing Entity; or
- (c) Non-Contractor software, modifications a Participating Entity/Purchasing Entity makes to, or any specifications or materials a Participating Entity/Purchasing Entity provides or makes available for, a Product; or
- (d) Participating Entity's/Purchasing Entity's combination of the Product or Service with a Non-Contractor product, data or business process; or damages based on the use of a Non-Contractor product, data or business process; or
- (e) Participating Entity's/Purchasing Entity's use of either Contractor's trademarks or the use or redistribution of a Product or Service in violation of this Master Agreement, Participating Addendum, or any other agreement incorporating its terms; or
- (f) Participating Entity's/Purchasing Entity's use of a Product or Service after Contractor notifies Participating Entity/Purchasing Entity to discontinue that use due to a third party claim.

(2) To qualify for such defense, the involved NASPO Participants (the "Indemnified Party") shall promptly notify the Contractor of any Intellectual Property Claim of which the Indemnified Party become aware which may give rise to right of defense pursuant to this Section. Notice of any Intellectual Property Claim that is a legal proceeding, by suit or otherwise, must be provided to Contractor within sixty (60) days of the Indemnified Party's learning of such proceeding. If the Indemnified Party's laws require approval of a third party to defend the Indemnified Party, the Indemnified Party will seek such approval and if approval is not received, Contractor is not required to defend that Indemnified Party. In the event the Indemnified Party does not authorize sole control to Contractor over any claims that may arise under this subsection, then the parties agree that Contractor will be granted authorization to equally participate in any proceeding subject to this subsection. The Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

If Contractor reasonably believes that a Product or Service may infringe or misappropriate a third-party's intellectual property rights, Contractor will seek to:

- i. procure for Participating Entities/Purchasing Entities the right to continue to use the Product or Service; or
- ii. modify or replace it with a functional equivalent to make it non-infringing and notify Participating Entities/Purchasing Entities to discontinue use of the prior version, which

Participating Entities/Purchasing Entities must do immediately.

If the foregoing options are not commercially reasonable for Contractor, or if required by a valid judicial or government order, Contractor may terminate Participating Entities'/Purchasing Entities' license or access rights in the Product or Service. In such a case, Contractor will provide Participating Entities/Purchasing Entities with notice and refund any amounts Participating Entities/Purchasing Entities have paid for those rights to the Product or Service.

THE FOREGOING SHALL CONSTITUTE THE LEAD STATE'S AND EACH AND EVERY PARTICIPATING AND/OR PURCHASING ENTITIES' SOLE REMEDY AND CONTRACTOR'S SOLE AND EXCLUSIVE LIABILITY FOR ALL INTELLECTUAL PROPERTY CLAIMS.

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, limits may be met in conjunction with primary and excess/umbrella insurance coverage;

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

(3) 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.

(a) 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

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

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

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

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

17. Laws and Regulations: Contractor will agree to comply with all Federal and State laws applicable to it as a corporation and as an IT Service Provider.

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

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

19. Ordering

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

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

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the

Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

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

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

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

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

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

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

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

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their

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

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

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

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

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

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

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

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

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

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

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

22. Data Access Controls:

a. Access Policy. Microsoft maintains a record of security privileges of individuals having access to Customer Data.

Access Authorization

- Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data.
- Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months.
- Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources.
- Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins.

b. Least Privilege

- Technical support personnel are only permitted to have access to Customer Data when needed.
- Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function.

c. Integrity and Confidentiality

- Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.
- Microsoft stores passwords in a way that makes them unintelligible while they are in force.

d. Authentication

- Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems.

- Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly.
- Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long.
- Microsoft ensures that de-activated or expired identifiers are not granted to other individuals.
- Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password.
- Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.
- Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

e. Network Design.

- Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access. Subject to further refinement in accordance with applicable Microsoft terms, 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:

a. Operational Policy. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

b. Data Recovery Procedures

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered.
- Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.

- Microsoft has specific procedures in place governing access to copies of Customer Data.
- Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months.
- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.

c. Malicious Software. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.

d. Data Beyond Boundaries

- Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks.
- Microsoft restricts access to Customer Data in media leaving its facilities.

e. Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

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.

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, Customer Data, or meta data may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

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

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master

Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

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

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

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

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

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

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

29. Title to Product: Reserved.

30. Data Privacy: Contractor must comply with all applicable laws related to data

privacy and security. Refer to Attachment E, Appendix A to the Microsoft NASPO VAluePoint Enterprise Agreement for Government Partners ("GPEA"), governing data privacy as applicable to Exhibit 1 to Attachment A Software as a Service, Exhibit 2 to Attachment A Platform as A service, and Exhibit 3 to Attachment A Infrastructure as a Service. The Contractor must comply with all applicable laws

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

- a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.
- b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.
- c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.
- d. The Contractor will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement.
- e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.
- f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

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

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

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

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

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

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

37. Governing Law and Venue

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

or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

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

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

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

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

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

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

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

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

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

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

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

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

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

identifier, may be submitted with any report.

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

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

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

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

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

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

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

d. The Limitation of liability in section 43 will not apply to claims for liability for damages caused by a party's (i) reckless misconduct, gross negligence, willful misconduct and/or fraud (provided that, in jurisdictions that do not recognize a legal distinction between "gross negligence" and "negligence," "gross negligence" as used in this subsection shall mean "recklessness"); (ii) liability for violation of its confidentiality obligations (except

obligations related to Customer Data) or the other party's intellectual property rights; or (iii) bodily injury or death.

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

Exhibit 1 to Attachment A of AR2473 Master Agreement: Software-as-a-Service

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

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

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

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. Refer to Attachment E GPEA, which governs data encryption.
- d. Reserved.
- e. The parties agree that: (1) metadata is owned and retained by Contractor; (2) no form of Customer Data or metadata is used for any purpose other than operating and supporting the Online Services; and (3) disclosure of Customer Data to law enforcement is subject to law, but is protected by Contractor according to the terms and conditions cited in both Appendix A and Appendix C to the GPEA and in the Microsoft Online Services Terms .
- 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: Certain In-Scope Services include both "Enterprise Plans" and "Government Plans." Such Government Plans may also be referred to as the "Government Community Cloud Services" offerings. As of the Effective Dates, Government Community Cloud Services Offerings, as identified in

the Product Terms and OST, include a subset of Office 365 Services, Azure Core Platform Services, and Dynamics CRM Online Services (each, as defined in the DPT).

A Purchasing Entity may be provisioned for either Enterprise Plans or Government Plans, but not as a mixture of both. Once a Purchasing Entity's tenant is provisioned either for Enterprise Plan(s) or Government Plans, it will remain so for the duration of the subscription term, including renewal terms. Purchasing Entity cannot migrate between these Plans.

As exceptions to the Foregoing

- (a) Customer Data will not be migrated between tenants by Microsoft pursuant to this Agreement (although in some cases Customer Data may be migrated pursuant to a separate, paid professional services agreement with Microsoft or another qualified company);
- (b) Each individual tenant may be provisioned either for Enterprise Plans or Government Plans, but not both; and
- (c) Purchasing Entity may not deploy or use Government Community Cloud Services and corresponding non-Government Community Cloud Services in the same domain.

All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights and this Amendment. Additionally:

- (i) Government Community Cloud Services will be offered only within the United States.
- (ii) Additional European Terms and the Standard Contractual Clauses, as set forth in the Use Rights, will not apply to Government Community Cloud Services.
- (iii) References to geographic areas in the DPT with respect to the location of Customer Data at rest, as set forth in the Use Rights, refer only to the United States.
- (iv) Notwithstanding the DPT section of the OST, Azure Government Services are not subject to the same control standards and frameworks as the Microsoft Azure Core Services. The Microsoft Azure Trust Center describes the control standards and frameworks with which Azure Government Services comply.

Specifically for the Government Community Cloud Services versions of the DPT Services Office 365 Services (Exchange Online, SharePoint Online, and Skype For Business Online, when sold as part of Office 365 for Government) and Dynamics CRM Online Services (Dynamics CRM Online Services for Government), the following shall apply:

- (i) Purchasing Entity Content is stored at rest in an encrypted form only within the United States.
- (ii) Access to Purchasing Entity Content by Microsoft Personnel who reside outside the United States, including access to Purchasing Entity Content by authorized support staff in identified support

centers, is prohibited except in very limited circumstances permitted by written Microsoft asset handling and access standards. Any such access permitted under the foregoing Microsoft standards shall occur only after commercially reasonable efforts have been made by Microsoft to perform the function necessitating Purchasing Entity Content access with employees who reside within the United States. (e.g. vacation or other specialist staff absence coverage). In cases when it occurs, all Purchasing Entity Content access granted shall provide the minimum access necessary, for the minimum time necessary, to Microsoft personnel who reside outside the United States. Further, Purchasing Entity shall be notified of each instance of this necessitated access by Microsoft Personnel who reside outside the United States.

(iii) Other than as permitted in subsection (ii), above, 24x7 support staff for Government Community Cloud Services outside the United States may access Customer Data, limited solely to the following: (1) names, email addresses and other contact information for Purchasing Entity's Tenant Administrators, and Purchasing Entity's domain names, will be made available to support staff; and (2) in some cases, Purchasing Entity personnel who contact such support staff may remotely display their screens to the support staff. All other types of Customer Data will only be accessed solely by US Persons. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

4. Security Incident or Data Breach Notification:

Contractor will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Contractor is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Contractor does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Security Incident Notification

If Contractor becomes aware of any unlawful access to any Customer Data stored on Contractor's equipment or in Contractor's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Contractor will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Contractor selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Contractor's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Contractor of any fault or liability with respect to the Security Incident.

Customer must notify Contractor promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

As an exception to the foregoing, notification of Security Incident will be delivered within 5 days after Contractor determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, the State must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

- 1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);
- 2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:
 - a. Name;
 - b. Title;
 - c. Email address registered as an administrator on the Online Services;
 - d. Email address not registered as a user on the Online Services;
- 3) Name of Purchasing Entity;
- 4) Enrollment number assigned by Contractor to represent Purchasing Entity's Tenant or Azure Subscription, on Offeror's subcontract with Contractor.

Contractor expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Contractor, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Additional language pertaining to reimbursements of costs:

To the extent that a Security Incident results from Contractor's failure to comply with its obligations under this Master Agreement (and, where applicable, Participating Addenda), and subject to the limitations of liability set forth in Attachment A, Section 43 (Limitation of Liability), Contractor will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's

obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Contractor's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Contractor under this paragraph will be characterized as direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the "EXCLUSION OF CERTAIN DAMAGES" in Attachment A, Section 43 (Limitation of Liability).

5. Personal Data Breach Responsibilities: Refer to Section 4 Security Incident or Data Breach Notification

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

8. Background Checks: Background checks will be governed by Section 8 of Attachment E to the GPEA.

9. Access to Security Logs and Reports: For the Online Services included in the Data Processing Terms section of the Microsoft Online Services Terms, Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Contractor shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity's Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change.

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

11. Data Center Audit:

Contractor Audits of Online Services

For each Online Service, Contractor will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Contractor's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Contractor's Confidential Information. The Microsoft Audit Report will clearly disclose any material

findings by the auditor. Contractor will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If a Purchasing Entity requests, Contractor will provide the Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Contractor's compliance with the security obligations under the Data Processing Terms (DPT) section of the Microsoft Online Services Terms. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Contractor and the auditor.

12. Change Control and Advance Notice: Contractor does not charge extra for new and updated features added to any given subscription-licensed "plan" for its Online Service. However, Microsoft may reasonably choose to create new license plans in order to monetize new features and functionality.

13. Security: Security requirements are governed by Section 8.B of Appendix A to the GPEA (Attachment E).

14. Non-disclosure and Separation of Duties: Non-disclosure and Separation of duties are governed by the Online Services Terms ("OST") included in the GPEA.

15. Import and Export of Data: Section 3 of Attachment E to the GPEA (Customer Data), shall govern the import and export of Data.

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 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:

Customer Data will be processed and retained intact for the duration of Customer's subscription (including data retention period defined in the Online Services Terms document) as described in

applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Contractor maintains multiple copies of Customer Data from which Customer Data can be recovered.
- Contractor stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.
- Contractor has specific procedures in place governing access to copies of Customer Data.
- Contractor reviews data recovery procedures at least every six months.
- Contractor logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.
- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Contractor will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Contractor shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Contractor customers and their data, or would compromise the security of the Office 365 Services, will be withheld. For clarity, "data restoration efforts" does not include automated Customer Data recovery processes such as when one of Contractor's datacenters is activated upon failure of another.

20. Compliance with Accessibility Standards: Compliance and Accessibility Standards shall be governed by section 8.A of Attachment E to the GPEA.

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: To whatever extent a form or use of encryption is required of Contractor pursuant to any of the industry and Federal government standards committed by Contractor in this Master Agreement and the Microsoft Online Services Terms, Contractor will comply with such requirements.

23. Subscription Terms: Subscription Terms shall be governed Section 8.G of Attachment E to the GPEA.

Exhibit 2 to Attachment A of AR2473 Master Agreement: Platform-as-a-Service

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

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

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

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. Refer to Attachment E GPEA, which governs data encryption.
- d. Reserved.
- e. The parties agree that: (1) metadata is owned and retained by Contractor; (2) no form of Customer Data or metadata is used for any purpose other than operating and supporting the Online Services; and (3) disclosure of Customer Data to law enforcement is subject to law, but is protected by Contractor according to the terms and conditions cited in both Appendix A and Appendix C to the GPEA and in the Microsoft Online Services Terms .
- 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: Certain In-Scope Services include both "Enterprise Plans" and "Government Plans." Such Government Plans may also be referred to as the "Government Community Cloud Services" offerings. As of the Effective Dates, Government Community Cloud Services Offerings, as identified in

the Product Terms and OST, include a subset of Office 365 Services, Azure Core Platform Services, and Dynamics CRM Online Services (each, as defined in the DPT).

A Purchasing Entity may be provisioned for either Enterprise Plans or Government Plans, but not as a mixture of both. Once a Purchasing Entity's tenant is provisioned either for Enterprise Plan(s) or Government Plans, it will remain so for the duration of the subscription term, including renewal terms. Purchasing Entity cannot migrate between these Plans.

As exceptions to the Foregoing

- (a) Customer Data will not be migrated between tenants by Microsoft pursuant to this Agreement (although in some cases Customer Data may be migrated pursuant to a separate, paid professional services agreement with Microsoft or another qualified company);
- (b) Each individual tenant may be provisioned either for Enterprise Plans or Government Plans, but not both; and
- (c) Purchasing Entity may not deploy or use Government Community Cloud Services and corresponding non-Government Community Cloud Services in the same domain.

All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights and this Amendment. Additionally:

- (i) Government Community Cloud Services will be offered only within the United States.
- (ii) Additional European Terms and the Standard Contractual Clauses, as set forth in the Use Rights, will not apply to Government Community Cloud Services.
- (iii) References to geographic areas in the DPT with respect to the location of Customer Data at rest, as set forth in the Use Rights, refer only to the United States.
- (iv) Notwithstanding the DPT section of the OST, Azure Government Services are not subject to the same control standards and frameworks as the Microsoft Azure Core Services. The Microsoft Azure Trust Center describes the control standards and frameworks with which Azure Government Services comply.

Specifically for the Government Community Cloud Services versions of the DPT Services Office 365 Services (Exchange Online, SharePoint Online, and Skype For Business Online, when sold as part of Office 365 for Government) and Dynamics CRM Online Services (Dynamics CRM Online Services for Government), the following shall apply:

- (i) Purchasing Entity Content is stored at rest in an encrypted form only within the United States.
- (ii) Access to Purchasing Entity Content by Microsoft Personnel who reside outside the United States, including access to Purchasing Entity Content by authorized support staff in identified support

centers, is prohibited except in very limited circumstances permitted by written Microsoft asset handling and access standards. Any such access permitted under the foregoing Microsoft standards shall occur only after commercially reasonable efforts have been made by Microsoft to perform the function necessitating Purchasing Entity Content access with employees who reside within the United States. (e.g. vacation or other specialist staff absence coverage). In cases when it occurs, all Purchasing Entity Content access granted shall provide the minimum access necessary, for the minimum time necessary, to Microsoft personnel who reside outside the United States. Further, Purchasing Entity shall be notified of each instance of this necessitated access by Microsoft Personnel who reside outside the United States.

(iii) Other than as permitted in subsection (ii), above, 24x7 support staff for Government Community Cloud Services outside the United States may access Customer Data, limited solely to the following: (1) names, email addresses and other contact information for Purchasing Entity's Tenant Administrators, and Purchasing Entity's domain names, will be made available to support staff; and (2) in some cases, Purchasing Entity personnel who contact such support staff may remotely display their screens to the support staff. All other types of Customer Data will only be accessed solely by US Persons. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

4. Security Incident or Data Breach Notification: Contractor will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Contractor is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Contractor does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Security Incident Notification

If Contractor becomes aware of any unlawful access to any Customer Data stored on Contractor's equipment or in Contractor's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Contractor will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Contractor selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Contractor's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Contractor of any fault or liability with respect to the Security Incident.

Customer must notify Contractor promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

As an exception to the foregoing, notification of Security Incident will be delivered within 5 days after Contractor determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, the State must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

- 1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);
- 2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:
 - a. Name;
 - b. Title;
 - c. Email address registered as an administrator on the Online Services;
 - d. Email address not registered as a user on the Online Services;
- 3) Name of Purchasing Entity;
- 4) Enrollment number assigned by Contractor to represent Purchasing Entity's Tenant or Azure Subscription, on Offeror's subcontract with Contractor.

Contractor expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Contractor, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Additional language pertaining to reimbursements of costs:

To the extent that a Security Incident results from Contractor's failure to comply with its obligations under this Master Agreement (and, where applicable, Participating Addenda), and subject to the limitations of liability set forth in Attachment A, Section 43 (Limitation of Liability), Contractor will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's

obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Contractor's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Contractor under this paragraph will be characterized as direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the "EXCLUSION OF CERTAIN DAMAGES" in Attachment A, Section 43 (Limitation of Liability).

5. Personal Data Breach Responsibilities : Refer to Section 4 Security Incident or Data Breach Notification.

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

8. Background Checks: Background checks will be governed by Section 8 of Attachment E to the GPEA.

9. Access to Security Logs and Reports:

For the Online Services included in the Data Processing Terms section of the Microsoft Online Services Terms, Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Contractor shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity's Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change.

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

11. Data Center Audit:

Contractor Audits of Online Services

For each Online Service, Contractor will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Contractor's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Contractor's Confidential Information. The Microsoft Audit Report will clearly disclose any material

findings by the auditor. Contractor will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If a Purchasing Entity requests, Contractor will provide the Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Contractor's compliance with the security obligations under the Data Processing Terms (DPT) section of the Microsoft Online Services Terms. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Contractor and the auditor.

12. Change Control and Advance Notice: Contractor does not charge extra for new and updated features added to any given subscription-licensed "plan" for its Online Service. However, Microsoft may reasonably choose to create new license plans in order to monetize new features and functionality.

13. Security: Security requirements are governed by Section 8.B of Appendix A to the GPEA (Attachment E).

14. Non-disclosure and Separation of Duties: Non-disclosure and Separation of duties are governed by the Online Services Terms ("OST") included in the GPEA.

15. Import and Export of Data: Section 3 of Attachment E to the GPEA (Customer Data), shall govern the import and export of Data

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, 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:

Customer Data will be processed and retained intact for the duration of Customer's subscription (including data retention period defined in the Online Services Terms document) as described in applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Contractor maintains multiple copies of Customer Data from which Customer Data can be recovered.

- Contractor stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.
- Contractor has specific procedures in place governing access to copies of Customer Data.
- Contractor reviews data recovery procedures at least every six months.
- Contractor logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.
- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Contractor will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Contractor shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Contractor customers and their data, or would compromise the security of the Office 365 Services, will be withheld. For clarity, "data restoration efforts" does not include automated Customer Data recovery processes such as when one of Contractor's datacenters is activated upon failure of another..

19. Compliance with Accessibility Standards: Compliance and Accessibility Standards shall be governed by section 8.A of Attachment E. to the GPEA.

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: To whatever extent a form or use of encryption is required of Contractor pursuant to any of the industry and Federal government standards committed by Contractor in this Master Agreement and the Microsoft Online Services Terms, Contractor will comply with such requirements.

22. Subscription Terms: Subscription Terms shall be governed Section 8.G of Attachment E to the GPEA.

Exhibit 3 to Attachment A of AR2473 Master Agreement: Infrastructure-as-a-Service

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

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

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

- a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.
- b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.
- c. Refer to Attachment E GPEA, which governs data encryption.
- d. Reserved.
- e. The parties agree that: (1) metadata is owned and retained by Contractor; (2) no form of Customer Data or metadata is used for any purpose other than operating and supporting the Online Services; and (3) disclosure of Customer Data to law enforcement is subject to law, but is protected by Contractor according to the terms and conditions cited in both Appendix A and Appendix C to the GPEA and in the Microsoft Online Services Terms .
- 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: Certain In-Scope Services include both "Enterprise Plans" and "Government Plans." Such Government Plans may also be referred to as the "Government Community Cloud Services" offerings. As of the Effective Dates, Government Community Cloud Services Offerings, as identified in

the Product Terms and OST, include a subset of Office 365 Services, Azure Core Platform Services, and Dynamics CRM Online Services (each, as defined in the DPT).

A Purchasing Entity may be provisioned for either Enterprise Plans or Government Plans, but not as a mixture of both. Once a Purchasing Entity's tenant is provisioned either for Enterprise Plan(s) or Government Plans, it will remain so for the duration of the subscription term, including renewal terms. Purchasing Entity cannot migrate between these Plans.

As exceptions to the Foregoing

- (a) Customer Data will not be migrated between tenants by Microsoft pursuant to this Agreement (although in some cases Customer Data may be migrated pursuant to a separate, paid professional services agreement with Microsoft or another qualified company);
- (b) Each individual tenant may be provisioned either for Enterprise Plans or Government Plans, but not both; and
- (c) Purchasing Entity may not deploy or use Government Community Cloud Services and corresponding non-Government Community Cloud Services in the same domain.

All terms and conditions applicable to non-Government Community Cloud Services also apply to their corresponding Government Community Cloud Services, except as otherwise noted in the Use Rights and this Amendment. Additionally:

- (i) Government Community Cloud Services will be offered only within the United States.
- (ii) Additional European Terms and the Standard Contractual Clauses, as set forth in the Use Rights, will not apply to Government Community Cloud Services.
- (iii) References to geographic areas in the DPT with respect to the location of Customer Data at rest, as set forth in the Use Rights, refer only to the United States.
- (iv) Notwithstanding the DPT section of the OST, Azure Government Services are not subject to the same control standards and frameworks as the Microsoft Azure Core Services. The Microsoft Azure Trust Center describes the control standards and frameworks with which Azure Government Services comply.

Specifically for the Government Community Cloud Services versions of the DPT Services Office 365 Services (Exchange Online, SharePoint Online, and Skype For Business Online, when sold as part of Office 365 for Government) and Dynamics CRM Online Services (Dynamics CRM Online Services for Government), the following shall apply:

- (i) Purchasing Entity Content is stored at rest in an encrypted form only within the United States.
- (ii) Access to Purchasing Entity Content by Microsoft Personnel who reside outside the United States, including access to Purchasing Entity Content by authorized support staff in identified support

centers, is prohibited except in very limited circumstances permitted by written Microsoft asset handling and access standards. Any such access permitted under the foregoing Microsoft standards shall occur only after commercially reasonable efforts have been made by Microsoft to perform the function necessitating Purchasing Entity Content access with employees who reside within the United States. (e.g. vacation or other specialist staff absence coverage). In cases when it occurs, all Purchasing Entity Content access granted shall provide the minimum access necessary, for the minimum time necessary, to Microsoft personnel who reside outside the United States. Further, Purchasing Entity shall be notified of each instance of this necessitated access by Microsoft Personnel who reside outside the United States.

(iii) Other than as permitted in subsection (ii), above, 24x7 support staff for Government Community Cloud Services outside the United States may access Customer Data, limited solely to the following: (1) names, email addresses and other contact information for Purchasing Entity's Tenant Administrators, and Purchasing Entity's domain names, will be made available to support staff; and (2) in some cases, Purchasing Entity personnel who contact such support staff may remotely display their screens to the support staff. All other types of Customer Data will only be accessed solely by US Persons. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.

4. Security Incident or Data Breach Notification: Contractor will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Contractor is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Contractor does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Security Incident Notification

If Contractor becomes aware of any unlawful access to any Customer Data stored on Contractor's equipment or in Contractor's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Contractor will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Contractor selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Contractor's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Contractor of any fault or liability with respect to the Security Incident.

Customer must notify Contractor promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

As an exception to the foregoing, notification of Security Incident will be delivered within 5 days after Contractor determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, the State must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

- 1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);
- 2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:
 - a. Name;
 - b. Title;
 - c. Email address registered as an administrator on the Online Services;
 - d. Email address not registered as a user on the Online Services;
- 3) Name of Purchasing Entity;
- 4) Enrollment number assigned by Contractor to represent Purchasing Entity's Tenant or Azure Subscription, on Offeror's subcontract with Contractor.

Contractor expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Contractor, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Additional language pertaining to reimbursements of costs:

To the extent that a Security Incident results from Contractor's failure to comply with its obligations under this Master Agreement (and, where applicable, Participating Addenda), and subject to the limitations of liability set forth in Attachment A, Section 43 (Limitation of Liability), Contractor will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's

obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Contractor's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Contractor under this paragraph will be characterized as direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the "EXCLUSION OF CERTAIN DAMAGES" in Attachment A, Section 43 (Limitation of Liability).

5. Personal Data Breach Responsibilities: Refer to Section 4 Security Incident or Data Breach Notification.

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

7. Termination and Suspension of Service:

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

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

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

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

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

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

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

8. Background Checks: Background checks will be governed by Section 8 of Attachment E to the GPEA

9. Access to Security Logs and Reports: For the Online Services included in the Data Processing Terms section of the Microsoft Online Services Terms, Event Logging. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity. Contractor shall allow Purchasing Entities reasonable self-service access to security information, latency data, and other related SaaS security data that affect this Contract and the Purchasing Entity's Data, at no cost to the Purchasing Entity. The parties recognize that the type of self-service access and security data made available to Purchasing Entities may be subject to change.

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

11. Data Center Audit: Contractor Audits of Online Services

For each Online Service, Contractor will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each Online Service.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Contractor's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Contractor's Confidential Information. The Microsoft Audit Report will clearly disclose any material

findings by the auditor. Contractor will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If a Purchasing Entity requests, Contractor will provide the Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Contractor's compliance with the security obligations under the Data Processing Terms (DPT) section of the Microsoft Online Services Terms. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Contractor and the auditor.

12. Change Control and Advance Notice: Contractor does not charge extra for new and updated features added to any given subscription-licensed "plan" for its Online Service. However, Microsoft may reasonably choose to create new license plans in order to monetize new features and functionality.

13. Security: Security requirements are governed by Section 8.B of Appendix A to the GPEA (Attachment E).

14. Non-disclosure and Separation of Duties: Non-disclosure and Separation of duties are governed by the Online Services Terms ("OST") included in the GPEA.

15. Import and Export of Data: Section 3 of Attachment E to the GPEA (Customer Data), shall govern the import and export of Data.

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 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:

Customer Data will be processed and retained intact for the duration of Customer's subscription (including data retention period defined in the Online Services Terms document) as described in applicable Online Services documentation published by Microsoft. Processing will be, in accordance with Customer instructions provided in this enrollment and provided through end user and administrator actions and inactions during the use of the services

Part 2: Data Recovery Procedures:

- On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Contractor maintains multiple copies of Customer Data from which Customer Data can be recovered.

- Contractor stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.
- Contractor has specific procedures in place governing access to copies of Customer Data.
- Contractor reviews data recovery procedures at least every six months.
- Contractor logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.
- In the event such Customer Data restoration activities are conducted and upon subsequent Customer request, Contractor will make the forgoing information from such logs available to the State, provided that: i) information will be provided only where it can be extracted from system wide logging with commercially reasonable efforts; ii) Contractor shall not be subject to an urgent timeframe for completion of the request (except as may be required by applicable law); and iii) any information in such logs which pertains to other Contractor customers and their data, or would compromise the security of the Office 365 Services, will be withheld. For clarity, "data restoration efforts" does not include automated Customer Data recovery processes such as when one of Contractor's datacenters is activated upon failure of another.

19. **Subscription Terms:** Subscription Terms shall be governed Section 8.G of Attachment E to the GPEA.

Attachment B: Scope of Services Awarded to Contractor

Contractor offers the following service models under this Master Agreement.

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
SaaS	X	X	X	See below
PaaS	X	X	X	See below
IaaS	X	X	X	

This document provides purchasing entities and eligible users a quick snap shot of the cloud solutions that Contractor provides.

Product	Category	Description
Azure Active Directory B2C	IaaS	Azure Active Directory, the cloud service with the proven ability to handle billions of authentications per day, extends its capabilities to manage consumer identities with a new service: Azure Active Directory B2C, now in public preview. Azure Active Directory B2C is a comprehensive, identity management solution for your consumer-facing applications that can be easily integrated to any platform, and accessible from any device. The service will be free during the public preview period.
Azure Active Directory	IaaS	Azure Active Directory provides identity management and access control for your cloud applications. To simply user access to cloud applications, you can synchronize on-premises identities, and enable single sign-on. Azure Active Directory comes in 3 editions: Free, Basic, and Premium.
Azure Active Directory Domain Services	IaaS	Azure Active Directory Domain Services provide scalable, high-performance, managed domain services such as domain-join, LDAP, Kerberos, Windows Integrated Authentication and Group Policy support. With the click of a button, administrators can enable managed domain services for virtual machines and directory-aware applications deployed in Azure Infrastructure Services. Built on the same underlying technology as Windows Server Active Directory, Azure Active Directory Domain Services provide an easy way to migrate traditional on-premises applications to the cloud.
Azure API Management	IaaS	Azure API Management lets you publish APIs to developers, partners, and employees securely and at scale.
Azure Application Gateway	IaaS	Azure Application Gateway is an Azure-managed layer-7 solution providing HTTP load balancing, SSL termination, and session-based cookie affinity to Internet-facing or internal web applications.
Azure App Service	PaaS	Azure App Service lets you create apps faster with a one-of-a kind cloud service to quickly and easily create enterprise-ready web and mobile apps for any platform or device and deploy them on a scalable and reliable cloud infrastructure.
Azure Automation	IaaS	Azure Automation lets you create, deploy, monitor, and maintain resources in your Azure environment automatically by using a highly scalable and reliable workflow execution engine.
Azure Backup	IaaS	On your corporate laptops, Azure Backup protects Windows client data and shared files and folders. In your datacenter, integrated with System Center Data Protection Manager (DPM), Backup protects Microsoft SharePoint, Exchange, SQL Server, Hyper-V virtual machines, and other applications.
Azure Batch	IaaS	Azure Batch makes it easy to run large-scale parallel and high-performance computing (HPC) workloads in Azure. Use Batch to scale out parallel workloads, manage the execution of tasks in a queue, and cloud-enable applications to offload compute jobs to the cloud.
Azure BizTalk Services	IaaS	Azure BizTalk Services is a powerful and extensible cloud-based integration service. It provides B2B and EAI capabilities for delivering cloud and hybrid integration solutions.
Azure Content Delivery Network	IaaS	Azure Content Delivery Network lets you deliver high-bandwidth content to users around the world with low latency and high availability via a robust network of global data centers.
Azure Cloud Services	IaaS	Azure Cloud Services removes the need to manage server infrastructure. With web and worker roles, it lets you quickly build, deploy, and manage modern applications.
Azure Container Service	IaaS	Azure Container Service is a container hosting environment optimized for Azure that lets you deploy, scale, and orchestrate container-based applications using Docker Swarm and Apache Mesos—popular, open source tools you’re already familiar with.
Azure Data Catalog	PaaS	Azure Data Catalog is a fully managed service that serves as a system of registration and system of discovery for enterprise data sources. It lets users—from analysts to data scientists to developers—register, discover, understand, and consume data sources. Use crowdsourced annotations and metadata to capture tribal knowledge within your organization, shine light on hidden data, and get more value from your enterprise data sources.
Azure Data Factory	IaaS	Azure Data Factory is a managed service that lets you produce trusted information from raw data in cloud or on-premises sources. Easily create, orchestrate, and schedule highly-available, fault-tolerant work flows of data movement and transformation activities. Monitor service health and all of your data pipelines at a glance with a rich visual experience offered through the Azure portal.
Data Lake analytics	PaaS	The Data Lake analytics service is a new distributed analytics service built on Apache YARN that dynamically scales so you can focus on your business goals, not on distributed infrastructure. Instead of deploying, configuring and tuning hardware, you write queries to transform your data and extract valuable insights. The analytics service can handle jobs of any scale instantly by simply setting the dial for how much power you need. You only pay for your job when it is running making it cost-effective. The analytics service supports Azure Active Directory letting you simply manage access and roles, integrated with your on-premises identity system. It also includes U-SQL, a language that unifies the benefits of SQL with the expressive power of user code. U-SQL’s scalable distributed runtime enables you to efficiently analyze data in the store and across SQL Servers in Azure, Azure SQL Database and Azure SQL Data Warehouse.
Data Lake Store	PaaS	The Data Lake store provides a single repository where you can capture data of any size type and speed simply without forcing changes to your application as the data scales. In the store, data can be shared for collaboration with enterprise-grade security. It is also designed for high-performance processing and analytics from HDFS applications (ie. Azure HDInsight, Data Lake analytics service, Hortonworks, Cloudera, MapR) and tools, including support for low latency workloads. For example, data can be ingested in real-time from sensors and devices for IoT solutions, or from online shopping websites into the store without the restriction of fixed limits on account or file size unlike current offerings in the market.
Azure DevTest Labs	PaaS	Azure DevTest Labs makes it easy to quickly create environments to deploy and test applications. Use reusable templates and artifacts to build Windows and Linux environments while minimizing waste and controlling costs.
Azure DNS	IaaS	Azure DNS lets you host your DNS domains alongside your Azure apps and manage DNS records by using your existing Azure subscription. Microsoft’s global network of name servers has the reach, scale, and redundancy to ensure ultra-fast DNS responses and ultra-high availability for your domains. With Azure DNS, you can be sure your DNS will always be fast and available.
Azure DocumentDB	IaaS	Azure DocumentDB is a fully-managed NoSQL document database service that offers querying and transaction-processing over schema-free data, predictable and reliable performance, and rapid development.
Azure Event Hubs	IaaS	Azure Event Hubs enables elastic-scale telemetry and event ingestion with durable buffering and sub-second end-to-end latency for millions of devices and events.
Azure ExpressRoute	IaaS	Azure ExpressRoute lets you create private connections between Azure datacenters and infrastructure that’s on your premises or in a colocation environment.
Azure HDInsight	IaaS	Azure HDInsight is a Hadoop-based service that brings an Apache Hadoop solution to the cloud. Gain the full value of big data with a cloud-based data platform that manages data of any type and size.
Azure HockeyApp	PaaS	HockeyApp lets you distribute beta versions, collect live crash reports, and get feedback from real users – all to enable you to build the world’s best mobile apps.
Azure IoT Hub	PaaS	Jumpstart your Internet of Things project with Microsoft Azure IoT Hub. Connect, monitor, and control millions of IoT assets running on a broad set of operating systems and protocols. Establish reliable, bi-directional communication with these assets, even if they’re intermittently connected, and analyze—and act on—incoming telemetry data. Enhance the security of your IoT solutions by using per-device authentication to communicate with devices that have the appropriate credentials. Revoke access rights to specific devices to maintain the integrity of your system.

Azure Key Vault	IaaS	Azure Key Vault offers an easy, cost-effective way to safeguard keys and other secrets in the cloud by using hardware security modules (HSMs). Protect cryptographic keys and small secrets like passwords with keys stored in HSMs. For added assurance, import or generate your keys in HSMs that are certified to FIPS 140-2 level 2 and Common Criteria EAL4+ standards, so that your keys stay within the HSM boundary. Key Vault is designed so that Microsoft does not see or extract your keys. Create new keys for Dev-Test in minutes and migrate seamlessly to production keys managed by security operations. Key Vault scales to meet the demands of your cloud applications without the hassle required to provision, <u>deploy, and manage HSMs and key management software.</u>
Azure Load Balancer	IaaS	Azure Load Balancer distributes Internet and private network traffic among healthy service instances in cloud services or virtual machines. It lets you achieve greater reliability and seamlessly add more capacity to your applications.
Azure Machine Learning	PaaS	Azure Machine Learning lets you easily design, test, operationalize, and manage predictive analytics solutions in the cloud.
Azure Managed Cache Service	IaaS	Azure Managed Cache Service is a distributed, in-memory, scalable solution that lets you build highly scalable and responsive applications by providing super-fast access to data.
Azure Media Services	IaaS	Azure Media Services offers cloud-based media solutions, including ingest, encoding, format conversion, content protection, and both on-demand and live-streaming capabilities.
Azure Mobile Engagement	PaaS	Azure Mobile Engagement lets you maximize mobile app usage and revenue. It's an SaaS-delivered, data-driven user-engagement platform that enables real-time, fine-grained user segmentation, app user analytics, and contextually-aware smart-push notifications and in-app messaging across all connected devices. It closes the marketing loop for app developers and marketers, letting them get directly in touch with all of their customers in a personal, contextually-aware, and non-intrusive way, and at the right time.
Azure Mobile Services	PaaS	Azure Mobile Services is a scalable cloud backend for building Windows Store, Windows Phone, Apple iOS, Android, and HTML/JavaScript applications. Store data in the cloud, authenticate users, and send push notifications to your application within minutes.
Azure Multi-Factor Authentication	IaaS	Azure Multi-Factor Authentication helps prevent unauthorized access to on-premises and cloud applications by providing an additional layer of authentication. Follow organizational security and compliance standards while also addressing user demand for convenient access.
Azure Notification Hubs	PaaS	Azure Notification Hubs is a highly scalable, cross-platform push notification infrastructure that lets you either broadcast push notifications to millions of users at once or tailor notifications to individual users.
Microsoft Office 365	SaaS	Subscription plans that include access to Microsoft Office applications plus other productivity services that are enabled over the Internet (cloud services).
Azure Operational Insights	IaaS	Azure Operational Insights lets you collect, correlate and visualize all your machine data, such as event logs, network logs, performance data, and much more, from both your on-premises and cloud assets.
Azure Redis Cache	IaaS	Azure Redis Cache—based on the popular open source Redis cache—gives you access to a secure, dedicated cache for your Azure applications.
Azure RemoteApp	IaaS	Azure RemoteApp helps employees stay productive anywhere, on a variety of devices—Windows, Mac OS X, iOS, or Android.
Azure Search	IaaS	Azure Search is a fully-managed service for adding sophisticated search capabilities to web and mobile applications without the typical complexities of full-text search.
Azure Security Center	IaaS	Azure Security Center helps you prevent, detect, and respond to threats with increased visibility and control over the security of all of your Azure resources. It provides a central view of security across your subscriptions and lets you set policies and monitor security configurations. Policy-driven recommendations guide resource owners through the process of implementing security controls and enable the rapid deployment of integrated Microsoft and partner solutions. Using Microsoft global threat intelligence, security-related events from across your Azure deployments are automatically collected and analyzed to identify actual threats and reduce false alarms. The resulting alerts offer insights into the attack and suggest ways to remediate issues.
Azure Service Bus	IaaS	Azure Service Bus is a messaging infrastructure that sits between applications allowing them to exchange messages for improved scale and resiliency.
Azure Service Fabric	PaaS	Service Fabric is a microservices platform used to build scalable, reliable, and easily managed applications for the cloud. Addressing the significant challenges in developing and managing cloud applications, Service Fabric allows developers and administrators to avoid solving complex infrastructure problems and focus instead on implementing mission-critical, demanding workloads.
Azure Site Recovery	IaaS	Azure Site Recovery helps you protect important applications by coordinating the replication and recovery of private clouds for simple, cost-effective disaster recovery.
Azure SQL Database	PaaS	Azure SQL Database is a relational database service that lets you rapidly create, extend, and scale relational applications into the cloud.
Azure SQL Data Warehouse	IaaS	Azure SQL Data Warehouse is an elastic data warehouse as a service with enterprise-grade features based on the massively parallel SQL Server processing architecture. It lets you scale data, either on-premises or in our cloud. It's the first cloud data warehouse that can dynamically grow or shrink, so you pay only for the query performance that you need, when you need it, up to petabyte-scale. SQL Data Warehouse lets you use your existing Transact-SQL (T-SQL) skills to integrate queries across structured and unstructured data. SQL Data Warehouse integrates with our data platform tools, including Azure HDInsight, Machine Learning, and Data Factory and Microsoft Power BI for a complete data-warehousing and business-intelligence solution in the cloud. With SQL Data Warehouse, you choose where to keep your data, either in the cloud or on-premises, based on your performance, security, and scale requirements.
Azure SQL Server Stretch Database	IaaS	With SQL Server Stretch Database, you can dynamically stretch warm and cold transactional data from Microsoft SQL Server to Azure. Unlike typical cold data storage, your data is always at hand. Stretch Database lets you provide longer data retention times than typical enterprise storage without breaking the bank. Depending on how often you'll access the data, choose the appropriate level of service, then scale up or down as needed. Using Stretch Database doesn't require any application changes. And you can use Stretch Database with new Always Encrypted technology, which helps protect your data at rest and in motion—extending data in a more secured manner for greater peace of mind.
Azure Storage	IaaS	Azure Storage offers non-relational data storage including Blob Storage, Table Storage, Queue Storage, and Files.
Azure StorSimple	IaaS	Azure StorSimple is a unique hybrid cloud storage solution for primary storage, archiving, and disaster recovery. StorSimple optimizes total storage costs and data protection. Note that the StorSimple 8000 Series is licensed separately from Azure services.
Azure Stream Analytics	IaaS	Azure Stream Analytics is an event-processing engine that helps you gain insights from devices, sensors, cloud infrastructure, and existing data properties in real-time. It's integrated out of the box with Event Hubs, and the combined solution can both ingest millions of events and do analytics to help you better understand patterns, power a dashboard, detect anomalies, or kick off an action while data is being streamed in real time.
Azure Traffic Manager	IaaS	Azure Traffic Manager lets you route incoming traffic across multiple hosted Azure services, whether they're running in the same datacenter or in different datacenters around the world.
Azure Virtual Machines	IaaS	Azure Virtual Machines lets you deploy a Windows Server or Linux image in the cloud. You can select images from a marketplace or use your own customized images.
Azure Virtual Network	IaaS	Azure Virtual Network lets you create private networks in the cloud with full control over IP addresses, DNS servers, security rules, and traffic flows. Securely connect a virtual network to on-premises networks by using a VPN tunnel, or connect privately by using the ExpressRoute service.
Visual Studio Application Insights	PaaS	Visual Studio Application Insights (in preview) is an all-in-one telemetry solution that can help you detect issues, triage impact and solve problems in your web apps and services. It provides deep diagnostics and real-time insights while being a seamless part of your ALM processes through Visual Studio, Visual Studio Team Services, and Azure Diagnostics integrations. It supports ASP.NET, J2EE and most of the popular web technologies for web apps on Azure or on your own servers.

Visual Studio Team Services	PaaS	Visual Studio Team Services is a cloud-based application lifecycle management (ALM) solution for everything from hosted-code repositories and issue-tracking to load-testing and automated builds. It's accessible from nearly anywhere, and you can create an account for free. Visual Studio Team Services is licensed separately from Azure services.
Azure VPN Gateway	IaaS	Azure VPN Gateway lets you establish secure, cross-premises connections between your virtual network within Azure and on-premises IT infrastructure.

Attachment C – Pricing Discounts and Pricing 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 % 18

Infrastructure as a Service Discount % 18

Platform as a Services Discount % 18

Value Added Services Discount % N/A

Additional Value Added Services:

All services required to set up the products proposed are included within the discounts offered for Software as a Service, Platform as a Service, and Infrastructure as a Service. CDW•G's Azure White Glove Service comes free of charge to our Azure customers.

Maintenance Services

Onsite Hourly Rate \$ N/A
Remote Hourly Rate \$ N/A

Professional Services

- Deployment Services Onsite Hourly Rate \$ N/A
Remote Hourly Rate \$ N/A
- Consulting/Advisory Services Onsite Hourly Rate \$ N/A
Remote Hourly Rate \$ N/A
- Architectural Design Services Onsite Hourly Rate \$ N/A
Remote Hourly Rate \$ N/A
- Statement of Work Services Onsite Hourly Rate \$ N/A
Remote Hourly Rate \$ N/A

Partner Services

Onsite Hourly Rate \$ N/A
Remote Hourly Rate \$ N/A

Training Deployment Services

Onsite Hourly Rate \$ _____ N/A _____

Online Hourly Rate \$ _____ N/A _____

Attachment D: Contractor's Response to Solicitation # CH16012



Table of Contents

ALL OTHER REQUIRED DOCS

1. Signature Page	
2. 5.4 Executive Summary	
3. Mandatory Minimums	
5.2 Cover Letter.....	3-2
5.3 Acknowledgement of Addendums	3-3
5.5 General Requirements	3-3
5.7 Recertification of Mandatory Minimums and Technical Specifications.....	3-5
3. Mandatory Minimums Attachments	
Acknowledgement of Amendments to RFP 2.3.....	1
Acknowledgement of Amendments to RFP 2.10.....	2
Microsoft SLAs	3
4. Business Information	
6.1 Business Profile.....	4-1
6.2 Scope of Experience	4-5
6.3 Financials	4-8
6.4 General Information.....	4-8
6.5 Billing and Pricing Practices	4-12
6.6 Scope and Variety of Cloud Services	4-17
6.7 Best Practices	4-20
4. Business Information Attachments	
Audited Financials 2013-2015.....	1
Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance.....	29
Subcontractors Authorized to Process Customer Data.....	49
5. Organization and Staffing	
7.1 Contract Manager	5-1

7. 3.13 Confidential, Protected or Proprietary Information

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

TECHNICAL PROPOSAL

6. Technical Requirements

8.1 Technical Requirements	6-3
8.2 Subcontractors	6-10
8.3 Working with Purchasing Entities	6-11
8.4 Customer Service	6-16
8.5 Security Information	6-17
8.6 Privacy and Security	6-20
8.7 Migration and Redeployment Plan	6-44
8.8 Service or Data Recovery	6-46
8.9 Data Protection	6-47
8.10 Service Level Agreements	6-50
8.11 Data Disposal	6-51
8.12 Performance Measures and Reporting	6-51
8.13 Cloud Security Alliance Questionnaires	6-56
8.14 Service Provisioning	6-56
8.15 Back Up and Disaster Plan	6-57
8.16 Solution Administration	6-62
8.17 Hosting and Provisioning	6-66
8.18 Trial and Testing Periods (Pre-and Post-Purchase)	6-70
8.19 Integration and Customization	6-71
8.20 Marketing Plan	6-72
8.21 Related Value-Added Services to Cloud Solutions	6-73
8.22 Supporting Infrastructure	6-75
8.23 Alignment of Cloud Computing Reference Architecture	6-76

6. Technical Requirements Attachments

Microsoft Online Service Terms	1
Microsoft Azure Security and Audit Log Management	33
Office 365 mapping of CDW Security, Compliance, and Privacy requirements	63
Standard Response to Request for Information Microsoft Azure Security, Privacy and Compliance	109
Attachment B: Exhibit 1	159
Microsoft SLAs	3

COST PROPOSAL

9. Cost Proposal

Attachment G – Cost Schedule	9-2
------------------------------------	-----





2. Executive Summary

Requirement

Offerors must provide an Executive Summary of its proposal. An Executive Summary should highlight the major features of an Offeror's proposal. Briefly describe the proposal in no more than three (3) pages. The evaluation committee should be able to determine the essence of the proposal by reading the Executive Summary. Any requirements that cannot be met by the Offeror must be included.

Response

NASPO ValuePoint has set out to establish a comprehensive cloud contract—one that will incorporate the industry's leading cloud service providers, the niche players, and even cloud products that have yet to be conceived. Your contract will span all three major service categories; it will protect the interests of participating entities, as they enjoy the financial benefits and flexibility that only cloud services offer. In order for you to create a contract that accomplishes so much, though, you had to include provisions that would be applicable to some offerings and not others. To this end, our response includes many clarifications. Please do not view these clarifications as an indication of inability to perform—rather, they are evidence of the care we have taken to ensure you have a complete understanding of the leading cloud provider, their offering, and how they conduct business through resellers.

Microsoft pioneered Software as a Service through Office 365, and Azure provides the industry's most trusted Platform and Infrastructure as a Service offerings. In our experience, Microsoft is one of the first cloud providers public sector customers request and the one they're most comfortable using to begin their foray into the cloud. As such, a Microsoft award is important to the success and widespread adoption of this contract. We have a long-standing relationship with Microsoft; we offer their full cloud suite; and we pride ourselves on offering the most accurate contractual and technical information available on Microsoft's cloud offering. For these reasons, where a provision is really more appropriate to other cloud providers but may have some applicability, we have taken care to explain how Microsoft's offerings meet the requirement or do not entirely apply to it. You will see that some of our responses are different from those of others proposing Azure and Office 365, likely including Microsoft itself. This is because our internal staff of cloud service specialists and contract specialists have extensive experience creating successful cloud contracts, and

they have lent their expertise to our response. We would welcome the opportunity to explain, in person and in greater detail, Microsoft's solution and how it fits into NVP's framework.



February 22, 2016

Christopher Hughes
Division of Purchasing
State of Utah

Solicitation No. CH16012 – NASPO ValuePoint Cloud Solutions

As of February, 2016 CDW holds the following MS authorizations:

- LSP (Licensing Solutions Provider) - allowing CDW to offer the Microsoft Enterprise and Select volume licensing program to end customers. The Enterprise licensing program includes all Microsoft Cloud Services and Microsoft Premier Product Support services.
- ADR (Authorized Device Reseller) – allowing CDW to offer Microsoft devices
- AER (Authorized Education Reseller) - allowing CDW to offer Microsoft academic products to education customers

In addition to reseller authorizations noted above, CDW is a **Microsoft Gold Certified Partner**. Microsoft Gold Certified Partners are elite Microsoft Business Partners who earn the highest customer endorsement. Microsoft Gold Certified Partners have passed the highest level of requirements from Microsoft and have demonstrated the most robust, efficient and scalable implementations of Microsoft technologies in demonstrated enterprise customer deployments or an on-site Microsoft assessment. CDW is a Gold Certified Partner in ten competencies, including:

- Microsoft Gold Certified Partner for Business Intelligence
- Microsoft Gold Certified Partner for Collaboration and Content
- Microsoft Gold Certified Partner for Communications
- Microsoft Gold Certified Partner for Devices and Deployment
- Microsoft Gold Certified Partner for Software Asset Management
- Microsoft Gold Certified Partner for Volume Licensing

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas O'Neil", written over a light gray background.

Thomas O'Neil
Director, US Public Sector Channel Program
Microsoft Corporation



3. Mandatory Minimums

5.2 Cover Letter

Requirement

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

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

Response

CDW•G provides the required cover letter below. We provide the signature pages as its own attachment to this response. Please see document titled "5.1 Signature Page CH16012 CDWG."



One CDW Way
230 N. Milwaukee Ave
Vernon Hills, IL 60061

P: 847.371.5800
F: 847.465.6800
Toll-Free: 800.808.4239

www.cdwg.com/PeopleWhoGetIT

07 March 2016

5.2 Cover Letter to the State of Utah's Solicitation CH16012, NASPO ValuePoint Master Agreement for Cloud Solutions

Dear Evaluators,

5.2.1 CDW Government LLC (CDW•G) understands that we may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

5.2.2 CDW•G is responsible for writing this proposal, with assistance from proposed solution manufacturer, Microsoft. The State can direction all questions regarding this response to Sr. Proposal Specialist Edie Harris via phone (312.705.6285) or email (ellharr@cdw.com).

5.2.3 CDW•G is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

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

5.2.5 The CDW•G proposed solutions include service models SaaS, IaaS, and PaaS. CDW•G is proposing Microsoft's Azure for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) and Microsoft's Office 365 Software as a Service (SaaS).

5.2.6 The Joint Authorization Board granted Azure and Azure Government a P-ATO at the Moderate Impact Level. Azure was the first public cloud with infrastructure and platform services to receive a P-ATO. The FedRAMP audit of Azure included the Information Security Management System that encompasses infrastructure, development, operations, management, and support of in-scope services. Other data available by NDA with Microsoft.

Confirmed by:

A handwritten signature in blue ink, appearing to read "Tara K. Barbieri".

Tara K. Barbieri, Director Program Sales and an individual authorized to commit the Offeror to the work proposed

5.3 Acknowledgement of Amendments (M)

Requirement

If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive. *Note: Offeror will not need to sign an amendment for a Master Agreement update. A Master Agreement update should be used when the action on the contract is objective and provides factual updates. Examples of when an update should be used in lieu of an Amendment include technical clarifications that do not change the SOW or Ts & Cs, e.g. changes of address, phone number, contact person, etc.*

Response

CDW•G acknowledges the release of ten amendments, the last of which was made on Feb 10, 2016 1:13:26 PM CST. We include the acknowledgement of amendment form on the pages following.

5.5 General Requirements (M)

Requirement

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.

Response

Yes, CDW•G agrees to provide quarterly sales reporting as described in the Master Agreement and any Participating Addendums. Program Manager, Jumana Dihy focuses support exclusively on our NASPO ValuePoint agreements and is intimately familiar with your reporting requirements. We provide more information on Jumana's expertise in the Organization Profile of our response.

Requirement

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.

Response

Yes, CDW•G agrees to cooperate with NASPO ValuePoint and SciQuest, if awarded. We have a dedicated team that deals only with integration and support for eProcurement. We have over 3,000 customers using Punch-out, Round trip or flat files catalogs. We currently have over 1,600 customers using SciQuest and have a strong working relationship with their integration team.

Requirement

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

Response

While CDW•G represents that all of Microsoft's CCMs were completed to the best of the knowledge of the authors thereof as of the time they were completed, CDW•G and Microsoft respectfully decline to represent and warrant the accuracy of CCMs. Additionally, for services that do not store or process sensitive Customer Data (e.g. applications such as Office 365 ProPlus, which is merely a delivery mechanism for on-premises software bits), Microsoft does not complete CCMs.

While the forms requested here do not apply to some of the cloud services we're offering, Microsoft does have a focus on security and invests in resources accordingly. Microsoft is represented on the Cloud Security Alliance Board of Directors by [Adrienne Hall](#), who is the General Manager for Issues & Crisis Management at Microsoft. She is an award-winning speaker on cloud computing, cybersecurity, and is a recurring author on the Microsoft Cyber Trust Blog. Hall also regularly meets with customers, law enforcement, and government agencies to share best practices for the protection of critical infrastructure and information technology systems.

Requirement

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

Response

CDW•G provides Microsoft's most recent SLA with our proposal, entitled Service Level Agreement for Microsoft Online Services March 1, 2016.

CDW•G is unable to negotiate Microsoft's SLA or submit to a Purchasing Entity's SLA requirements due to corporate policies surrounding the operational and security controls of Microsoft's cloud service. For clarity, Microsoft's SLAs are administered in a consistent and, in some cases, automated way for all its customers, and may therefore not be customized. For any given cloud service, the SLA in effect as of the time a subscription order is first placed is locked and will not change during the term of a subscription order. Upon renewal of a Purchasing Entity's subscription order, Microsoft's then-current SLA will supersede the previous SLA. The Purchasing Entity's renewal of its subscription will constitute its written approval of the then-current (new) SLA.

Microsoft's historical practice has been to improve its SLAs over time and have never before adversely changed any SLA terms. However, Microsoft's SLAs may not be customized for

any customer, and they must reserve the right to change SLAs over time at their discretion, except to the extent one is locked for a subscription as noted above.

5.7 Recertification of Mandatory Minimums and Technical Specifications

Requirement

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 mandatory minimum requirements and technical specifications of the RFP.

Response

CDW•G agrees, to the extent as detailed in the following Clarifying Statement:

Please note the extent to which Microsoft has taken exception and/or provided disclaimers to the terms and conditions of the RFP. All technical specifications and features/functions are subject to change. That said, the core feature and security and privacy commitments made in Microsoft's Online Services Terms (OST) document (which will be incorporated by reference into both the subcontract and the terms and conditions Microsoft will require CDW•G to flow up to its customers) will be locked in place for the term of any subscription order during the 10-year term, based upon the version of the OST in effect as of the date of the initial order for that subscription (subscription orders are typically for 3 years at a time). CDW•G and Microsoft will meet annually to discuss any changes to the OST. Microsoft strives to improve its features, functionality, and related terms and conditions, does not anticipate any negative changes.





5. Organization Profile

Expert contract support is a hallmark of CDW·G's **program management team**. Most vendors—even large resellers—neglect to have a team devoted to managing their contracts, instead relying on salespeople for compliance and reporting issues, which can result in delayed responses, unreliable support, and potentially faulty reporting. CDW·G, however, understands that contracts are serious commitments, and we honor these commitments through our dedicated program management team. Information pertaining to the contract manager, **Jumana DiHu**, is included on the following pages.

7.1 Contract Manager (ME)

Requirement

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

Response

Expert contract support is a hallmark of CDW·G's **program management team**. Most vendors—even large resellers—neglect to have a team devoted to managing their contracts, instead relying on salespeople for compliance and reporting issues, which can result in delayed responses, unreliable support, and potentially faulty reporting. CDW·G, however, understands that contracts are serious commitments, and we honor these commitments through our dedicated program management team. Information pertaining to our NASPO ValuePoint contract manager, **Jumana DiHu**, is included on the following pages.

Requirement

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.

Response

- Jumana DiHu, Program Manager
- **Phone:** 312.547.2495
- **Email:** jumdihu@cdwg.com
- **Work Hours:** 8am–5pm CST

Requirement

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.**

Response

Ms. Dihu has over a decade of contract management experience and has been supporting our NASPO ValuePoint reseller agreements for over two years. She is currently responsible for a full range of contracts which face CDW•G customers and partners (e.g., Master Purchase Agreements, Subcontractor Agreements, Reseller Agreements, etc.). She is practiced in initiating and responding to requests for contract changes, product substitutions, and technical refreshments, and facilitates preliminary dispute resolution, ensures and documents compliance, and educates and assists the sales teams with contract terms and deliverables.

Prior to joining CDW•G, Ms. Dihu spent 11 years as a program manager for Sirva, Inc., specializing in contract negotiation, cost/price analysis, compliance, market and channel analysis, and development of strategic initiatives. She received her degree in International Economics from DePaul University in Chicago. Her resume is included at the end of this section.

Requirement

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.

Response

Ms. Dihu will oversee the NASPO ValuePoint Cloud contract details post-award, including issuing reports, audits, and providing overall program and contract management. Per our best practices, her management of the NASPO Value Point contracts includes three key areas: reporting, compliance, and education. Those key areas constitute the responsibilities fulfilled by Ms. Dihu as the NASPO ValuePoint Cloud contract manager, and are described as follows:

Reporting

Whether NASPO ValuePoint customers require reports to make budgeting simpler, to keep track of assets, or to understand purchasing trends, they need the vendor community to submit reports promptly and in the correct format. CDW•G is consistently lauded for its comprehensive and accurate reporting. We have built specialized software to automate many aspects of the reporting process. The reports that we currently generate run the gamut from highly manual, daily reports to automated, annual reports for customers at the local government level. Not only will participating NASPO ValuePoint agencies experience

less downtime as a result of CDW•G's on-time reporting standards, they benefit from regular business reviews presented by the program manager based upon the data being reported.

Compliance

Immediately upon award of a contract, Ms. DiHu reads the contract documents and all related proposal documents, recording all items that CDW•G will need to manage. Ms. DiHu is responsible for ensuring that CDW•G observes all legal statutes included in the contract as well as all business commitments. For example, if CDW•G commits to a pricing structure based on a certain discount from advertised pricing, it is the program manager's responsibility to record the pricing in the contract management software, which then locks the structure for purchases made under the contract. Since the program manager is often the person most familiar with the contract, she will also make recommendations for improvements and efficiencies based upon her constant analysis of the contract's provisions and trends in agency usage of the contract.

Education

The program manager is also responsible for promoting the contract to all potential end users and reminding them of the benefits of purchasing via the Master Agreement and/or Participating Addenda already negotiated as part of the NASPO ValuePoint Cloud contract. The program management team will conduct trainings internally to educate sales representatives about the requirements of the contract. Subsequent follow-up training is conveyed via email, and an internal website provides training decks, marketing material, frequently asked questions, and important contact information for sales coworkers.

More information about how this contract is marketed to interested agencies is included in our **Technical Response**.



6. Technical Response

A. Narrative

Requirement

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

Response

Traditional IT operations required a data center and data centers were required because IT services and applications became “critical” to the business and needed to be protected. To protect those applications and services an environment that was cool, humidity controlled and static free was required. Conditioned power that was backed-up with UPS systems and generators were also needed so if the power company suffered a failure from a storm or some other event, the data center and the business continued to operate.

The number of “business critical” applications, whether actually “critical” or not, ballooned and the test/development environment grew with every infrastructure life-cycle purchase. The amount of expensive environmentally controlled floor space required continued to increase. While virtualization technologies brought efficiencies to the server infrastructure, data centers still needed to be expanded or new ones had to be built. Building data centers is very expensive, particularly when there are requirements for business continuity/disaster recovery in secondary locations. With the amount of budget required to support IT operations it is little wonder that the hardest part of a CIO’s job becomes making the business case for IT. So how does a CIO meet the IT needs of the business in the most cost-effective manner? Is it expanding the on-premises data center footprint, co-location in 3rd party data centers, Private Cloud, Public Cloud, or Hybrid Cloud?

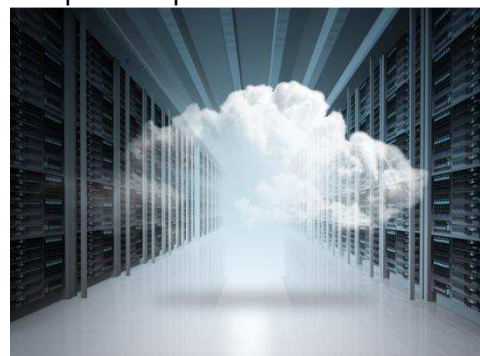


Figure 1: Which Cloud model is the most cost-effective choice for meeting your business needs? (photo source: iStock)

In government, Cloud computing is a relatively new possibility. Previously, IT capabilities were always delivered from on-premises data centers or leased co-location space service as an extension of on-premises facilities. With a programmatic approach to security concerns in place (FedRAMP, HIPPA, CJIS), it's now possible to have some government IT services delivered from a multi-tenant cloud services provider, bringing with it a host of possibilities. There are cost savings and efficiencies versus traditional infrastructure but also relief for resource constrained data centers, cap-ex avoidance for facility upgrades, facility and personnel resources for new initiatives, consolidation of data centers and savings from actually being able to turn down portions of a data center. While the promise of cost savings and efficiencies is real and achievable, cloud is not the answer for every IT service. Placing the wrong IT service in the cloud can have serious consequences, the least of which could be wasted time and money. The question then is which of your IT services can or should be delivered from the Cloud? The full answer to this question is different for every enterprise.

In government and other areas where on-premises has been the norm, it is important to carefully assess where cloud is the right fit for a given IT service. Our recent data from commercial IT leaders indicates 1/3 of IT professionals we surveyed have either moved something back to on-premises from the cloud or are planning to. This demonstrates the importance of having a technology partner like CDW•G who will help customers identify the best IT delivery model for a given IT service. A technology partner will help identify what in the IT environment is best suited to a cloud service, which type of cloud service and which cloud service provider is the proper fit for each unique requirement.

Identifying what is not a good fit for the cloud is equally important in order to avoid what 1/3 of the IT professionals we surveyed are experiencing. Finally, the only reason to do any of this is to achieve cost savings and efficiencies. Showing the savings is critical. The savings includes cost avoidance of infrastructure purchases but it's much more than that and it usually spans multiple budgets. It's about facility savings, as well. Data Centers are wildly expensive to build and to maintain. They are built, outfitted and maintained based on the totality of the IT services the data center needs to support. When portions of data centers can be decommissioned or turned-down (because some IT services are now in the cloud) there are real savings. When data center expansions or builds can be avoided altogether, there are tremendous savings. When new IT services can be added because the facility and/or personnel resources can now support it, the organization is no longer stymied. A partner with a full-range of cloud services capabilities can be an invaluable resource to an organization seeking the cost savings and efficiencies that the cloud can bring.

B. Point-by-Point Response

Requirement

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

Response

CDW•G acknowledges this requirement and have not provided links to websites as part of our response to the requirements within this section.

8.1 Technical Requirements (M) (E)

Requirement

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**.

Response

CDW•G is proposing Microsoft's Azure for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) and Microsoft's Office 365 Software as a Service (SaaS). Office 365 is a subscription service that combines the familiar Microsoft Office suite with cloud-based versions of Microsoft's next generation communication and collaboration services.

Microsoft Windows Azure is an internet-scale, high-availability cloud fabric operating on globally-distributed Microsoft data centers. Windows Azure and related tools support the development and deployment of applications into a hosted environment that extends the on-premises data center.

Microsoft Azure Government is a government-community cloud that offers hyper-scale compute, storage, networking, and identity management services, with world-class security. A physically and network-isolated instance of Microsoft Azure, operated by screened U.S. citizens, Azure Government provides standards-compliant IaaS and PaaS that has now received a FedRAMP JAB P-ATO. All services are available immediately for supporting secure US government workloads, including CJIS, IRS 1075 FTI, HIPAA, DoD, and federal agency data.

CDW•G provides the following Clarifying Statement from Microsoft, in regards to the solutions proposed:

The Microsoft Online Services in this Proposal provide highly-scalable and configurable solutions to address each Purchasing Entity's stated business needs in a cost-effective manner. These Online Services are multi-tenant "cloud" solutions hosted by Microsoft, operating on standardized terms, protocols and procedures. Microsoft is not able to customize the Online Services or their operational protocols for any individual government customer.

As with any standardized cloud service, Offeror's subcontractor, Microsoft, expects to evolve and improve the features and functions of these Online Services. For that reason, Microsoft reserves the right to update and change features and functionality described in this response during the term of the agreement between parties.

The features and functionality listed in the Proposal represent the Microsoft Online Services as of our response date, but neither CDW•G nor Microsoft can guarantee that these features and functions will not change over time. Microsoft generally provides advance notice to its customers of major changes, but might not in all cases notify regarding minor changes. It is Microsoft's goal to improve the service over time.

Requirement

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

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

Response

Microsoft Windows Azure is an internet-scale, high-availability cloud fabric operating on globally-distributed Microsoft data centers. Windows Azure and related tools support the development and deployment of applications into a hosted environment that extends the on-premises data center.

On-demand self-service refers to the service provided by Microsoft Azure that enables the provision of resources on demand whenever required. In on-demand services can be enabled from the HTML Portal, using Azure API, using CLI for Mac, Linux, and Windows with Azure Service Management. Azure on-demand self-service resource sourcing programmatically is a prime feature allowing the user to scale the infrastructure.

Requirement

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.

Response

Microsoft Azure enables the enterprise to create an on-premises network route from on-premises VPN device and the Azure virtual network.

- Configure on-premises hardware or software VPN device to terminate the VPN tunnel, which uses Internet Protocol security (IPsec)
- Gateway connects on-premises to Microsoft Azure through many connection bandwidth using software only or hardware based connectivity
- Basic VPN connection, Standard VPN, ExpressRoute gateway connections
- Create internal Microsoft Azure virtual network to support separation of site resources or sharing of information and subscription to subscription connection

Requirement

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.

Response

Azure resource pooling supports scalable systems involved in cloud computing and software as a service (SaaS), enable “near” infinite growth with immediately availability. The kinds of services that can apply to a resource pooling strategy include data storage services, processing services, bandwidth provided services and other azure related compute elasticity.

Requirement

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.

Response

Microsoft Azure supports rapid elasticity allowing automated requests additional resources (i.e. compute, disk space, connectivity and other types of services). Microsoft Azure services are allocated and de-allocated resources irrelevant to the client or user's side. Microsoft Azure provides resources appear to be “nearly” infinite with automatic availability.

Requirement

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.

Response

Microsoft Azure supports NIST principles areas of measured services such as measured service setup allowing Azure systems to control a system, user or tenant's usage of resources with metering capability. Azure supports automated remote services measurement tools to provide auditing and accountability of utilization. Azure measured service ensures that even when there is no specific interaction for a service change, that service change is still audited to support billing cycles.

Requirement

8.1.3 Offeror must identify for each service category(ies) the areas that each service category. 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.

Response

The RFP list of many (not all) service category are listed in Attachment D.

NIST SP 800-145 defines Infrastructure-as-a-Service (IaaS) as “*The capability provided to the consumer is 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, and deployed applications; and possibly limited control of select networking components.”

Deploying an application and managing an IaaS environment provides the most flexibility that Azure has to offer. With any deployment choice, there will be pros and cons that must be considered. The greatest benefit of an IaaS implementation is that it offers the greatest amount of control from the operating system to manage access to the application.

IaaS is most like traditional IT delivery. Customers provision their own virtual machines, define their own networks, and allocate their own virtual hard disks. IaaS shifts the burden of operating datacenters, virtualization hosts, and hypervisors. In addition, the business continuity and disaster recovery infrastructure is shifted from the enterprise to the service provider.

NIST SP 800-145 defines Platform-as-a-Service (PaaS) as *“The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. 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 configuration settings for the application-hosting environment.”*

With PaaS applications, many of the layers of management are removed and more flexibility is provided than an application running on IaaS instances. Specifically, there is no need to manage the operating system, including patching, which reduces some of the complexity of designing the deployment.

A significant benefit of deploying an application running in a PaaS environment is the ability to quickly and automatically scale up the application to meet the demand when traffic is high, and inversely scale down when the demand is less. Deploying an application in the PaaS model is very cost effective from a scalability and manageability perspective.

PaaS extends IaaS further by providing multitenant services that customers subscribe to. Platform services are a transformational computing model that can dramatically reduce the costs and increase the agility of delivering applications to end users internally and externally. PaaS users bring their own application code but leverage robust platforms, which they do not need to maintain.

NIST SP 800-145 defines Software-as-a-Service (SaaS) as *“The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either 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.”

Choosing an Azure SaaS offering provides the least amount of responsibility on the customer's side. At the same time, providing a lesser amount of flexibility in comparison with an IaaS or PaaS approach.

SaaS is the real promise of cloud computing. By integrating applications from one or multiple vendors, customers need to bring only their data and configurations. They can eliminate the costs of building and maintaining applications and platform services and still deliver the secure, robust solutions to the end users.

Many scenarios need to implement a blend of Azure offerings to meet the needs of their organization and application requirements. The following diagram highlights the main differences from a manageability perspective, when using public cloud SaaS, PaaS, IaaS and On-Premises implementations:

	SaaS	PaaS	IaaS	On Prem
Applications				
Data				
Runtime				
Middleware				
Operating System				
Virtualization				
Servers				
Storage				
Networking				
Physical Datacenter				
	 Microsoft		 Customer	

Requirement

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

Response

CDW•G is willing to comply with the requirements of Attachments C & D, to the extent as detailed in the following Clarifying Statement:

NIST Special Publication 800-145 is a set of definitions, general characteristic and recommendations for cloud services, but was not intended by NIST as a control set or framework for "Compliance." Not all cloud services can be expected to conform to all of the characteristics outlined therein.

CDW•G, on behalf of its subcontractor, Microsoft, will agree that, during the term of a Purchasing Entity's subscription for its "Government Community Cloud Services" (as defined in Microsoft's terms and conditions), those services will be operated in accordance with a written data security policy and control framework that is consistent with the requirements of NIST 800-53 Revision 4, or successor standards and guidelines (if any), established to support Federal Risk and Authorization Management Program (FedRAMP) accreditation at a Moderate Impact level. Microsoft intends for Government Community Cloud Services to support FedRAMP Authority to Operate (ATO), and Microsoft will use commercially reasonable efforts to obtain an ATO from a Federal agency, and to maintain such ATO through continuous monitoring processes and by conducting regular FedRAMP audits.

Additional information regarding Microsoft's compliance and adherence to other standards, such as CJIS, IRS 1075, HIPAA, FERPA, ISO/IEC 27001 and 27018, SOC1 and 2, and others can be found on the online Microsoft Trust Center.

Also, please refer to our Exception and Clarifying Statements for Attachment A, Section 17. Please note that some of these standards apply only to certain services (e.g. CJIS applies only our Government Community Cloud services) and that some of them require special Amendments and/or Agreements (e.g. CJIS requires that a State's CJIS Systems Agency must execute a special agreement with Microsoft, before Microsoft will provide an FBI CJIS Addendum for use in each such state). Microsoft welcomes the opportunity to discuss this in more detail during negotiation.

Additionally, for the commercial and education versions of DPT services which are not Government Community Cloud Services, each such DPT Service follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below.

MICROSOFT Online Services in DPT	
Microsoft Dynamics CRM Online Services	Microsoft Dynamics CRM Online services made available through volume licensing or the Microsoft online services portal, excluding (1) Microsoft Dynamics CRM for supported devices, which includes

MICROSOFT Online Services in DPT	
	but is not limited to Microsoft Dynamics CRM Online services for tablets and/or smartphones and (2) any separately-branded service made available with or connected to Microsoft Dynamics CRM Online, such as Microsoft Social Engagement, Parature, from Microsoft, and Microsoft Dynamics Marketing.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Exchange Online, Exchange Online Archiving, Exchange Online Protection, Advanced Threat Protection, SharePoint Online, OneDrive for Business, Project Online, Skype for Business Online, Sway, Office Online, Delve Analytics, Customer Lockbox, and Yammer Enterprise. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded "for Office 365."
Microsoft Azure Core Services	Cloud Services (web and worker roles), Virtual Machines (including with SQL Server), Storage (Blobs, Tables, Queues), Virtual Network, Traffic Manager, Batch, Web Sites, BizTalk Services, Media Services, Mobile Services, Service Bus, Notification Hub, Workflow Manager, Express Route, Scheduler, Multi-Factor Authentication, Active Directory, Rights Management Service, SQL Database, and HDInsight.
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.

Microsoft has instructed Offeror to paste a table into its response. The table is shown at the top of this document, and may be found at the Microsoft Online Services Terms (which are to be incorporated by reference into the subcontract and Master Agreement) in the section of the OST titled "Online Services Information Security Policy." Microsoft may add or remove services from this table (via updates to the OST) in the future, although removals are highly unlikely.

The Microsoft Amendment M306 (the Government Community Cloud Services Amendment) is also included with the Microsoft-required terms.

Requirement

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**.

Response

CDW•G has provided this information in Response 8.1.4 above.

8.2 Subcontractors (E)

Microsoft makes strong contractual commitments to safeguard Customer Data and provide privacy protections. This includes provisions for customers in geographies or industries with additional controls around personal data.

Microsoft may hire other companies to provide limited services on its behalf, such as providing customer support. Microsoft will only disclose Customer Data to subcontractors so that they can deliver the services we have retained them to provide. Subcontractors are prohibited from using Customer Data for any other purpose, and they are required to maintain the confidentiality of our customers' information.

Microsoft requires subcontractors to join Microsoft's Supplier Security & Privacy Assurance Program, to meet their privacy requirements by contract, and to undergo regular privacy training. They contractually obligate subcontractors that work in facilities or on equipment controlled by Microsoft to follow our privacy standards. All other subcontractors are contractually obligated to follow privacy standards equivalent to their own.

Requirement

8.2.1 Offerors are asked to 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.

Response

In the sense that NASPO has defined the term Subcontractor—"any organization...that will assist an Offeror to provide an Offering if awarded a Master Agreement"—Microsoft will be CDW•G's. As a cloud service provider, Microsoft will be responsible for providing all the services described within this proposal, and, as such, NVP end users will execute agreements directly with Microsoft, naming CDW•G as the billing partner. We have included Microsoft's clarifications and exceptions within this proposal.

Microsoft is among the industry's most qualified to offer cloud services. In terms of data security, breadth of offerings, and past performance, there are few cloud service providers as accomplished and trusted as Microsoft. Our proposal describes in detail Microsoft's qualifications and ability to meet NASPO's Administrative, Business, and Technical Requirements, including clarifications where necessary.

Microsoft and its affiliates operate Microsoft Azure Services. Microsoft may hire other companies to provide limited services on its behalf. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

Requirement

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.

Response

Microsoft will perform the contract requirements and CDW•G will bill for Microsoft's cloud services. We anticipate that Microsoft and NASPO will negotiate a Master Agreement directly and that CDW•G will be named within it as Microsoft's billing partner.

Requirement

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.

Response

As noted above, CDW•G's subcontractor, Microsoft, is among the industry's most qualified to offer cloud services to public sector customers. This proposal expounds upon those qualifications. Microsoft will not accept flow-down of Statement of Work requirements.

8.3 Working with Purchasing Entities (E)**Requirement**

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 (refer to the persons/roles identified in Section 7);
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

Response

Microsoft Operations Centers (MOCs) are globally distributed and work around the clock in a "follow-the-sun" model to ensure our cloud services are persistently available. Each MOC is staffed with a team of incident management professionals and collectively they are responsible for monitoring service health, process automation, infrastructure operations, event and crisis management, and communications across the business.

They are responsible for more than five hundred service components and monitor the servers and devices for the services Microsoft provides. Most critically, this is the team that identifies and resolves service incidents and outages when things go wrong.

In an environment with so many services, not all incidents are the same. Over half of all incidents are handled through automation and 90 percent of all incidents are handled at first touch. The most severe issues are resolved by a highly trained and qualified crisis

management team, working on technical resolution, escalations, and communications to the impacted business groups.



For more information, please refer to our response to 8.6.8 Security Incident Notification.

CDW•G also provides the following Clarifying Statement from Microsoft, in regards to the solutions proposed: Microsoft has taken exception to the RFP’s language for Data Breach (a.k.a. Security Incident) responses, since Microsoft uses standard rules and methodology that is not subject to negotiation of customer-written terms and conditions. Most importantly for purposes of this Section 8.31(e), as of today (although this may change in the future) Microsoft only notifies one or more persons that are assigned to the role of “global administrator” in the Administrative Portal of the Online Services. This means that if an Offeror employee is not one of the global administrators, then CDW•G will not be notified by Microsoft of the Security Incident. And if both CDW•G and Customer personnel are jointly listed as global administrators, then there is a chance that only a Customer administrator (and not an Offeror administrator) will be notified, since Microsoft may not notify all administrators if one has already responded. That said, whether Microsoft notifies the Customer directly or notifies CDW•G (so that CDW•G may notify the customer), there is no reason why the Customer should not be notified timely of any Security Incident (as per Microsoft’s contractual commitment).

Requirement

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.

Response

CDW•G acknowledges that it will not engage nor permit CDW Government LLC agents/employees to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement. As a reseller for a long list of NASPO

ValuePoint agreements, we are well versed in this requirement. We will continue to follow the guidelines that you have set for the Cloud contract as well.

Requirement

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

Response

CDW•G asserts the following:

- a. CDW•G subcontractor, Microsoft, currently, as of the date of the Proposal, has a mechanism by which 30-day Trial subscriptions may be ordered for some, but not all, of the cloud services offered hereunder. Microsoft will provide additional information about this upon request of Lead State, Participating States, or any Purchasing Entity.
- b. It is possible for any Purchasing Entity to purchase a separate subscription for the purpose of establishing a second environment for test and/or staging purposes. Such separate Subscription would be at an additional cost, and additional contract paperwork may be required.

Requirement

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

Response

CDW•G takes great pride in our ability to provide end users with the right technology, right away. At CDW•G we make accessibility to technology a top priority. We believe that all people should have fair and equitable access to technology resources. We do this in accordance with US Section 508. As we offer commercially available, off the shelf products, NASPO ValuePoint can be assured our manufacturer partners products' hold these

capabilities. CDW•G proudly offers a variety of assistive products specifically designed to provide accessibility to individuals who have physical or cognitive difficulties, impairments, and disabilities.

CDW•G proves our commitment to serving users with disabilities with our own tools, technologies and resources. For example, the CDW•G iPhone Application allows those customers with mobility disabilities to search, view and order products by using a touch screen instead of sitting at a desk, using a standard mouse and keyboard. For further ease of use, this application functions with the accessibility features of the phone and available assistive technology. Like the manufacturers of the products we offer, CDW•G has a proven record of rising to meet the needs of all customers.



Offeror's subcontractor, Microsoft, complies with all laws applicable to it as IT service provider, but not laws applicable to a Purchasing Entity's own operations. Microsoft's research indicates that most if not all State accessibility laws (and the Federal ADA) applies to our customers (and not to Microsoft, as service provider), so Offeror respectfully takes exception with this clause, as written. Microsoft supports the government's obligation to provide accessible technologies to its citizens with disabilities as required by Section 508 of the Rehabilitation Act of 1973, and its state law counterparts (including applicable California provisions). Offeror encourages Purchasing Entities to judiciously compare product accessibility performance. The Voluntary Product Accessibility Templates ("VPATs") for the Microsoft technologies used in providing the online services can be found at Microsoft's VPAT page.

Requirement

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

Response

For each of the Microsoft cloud services offered by CDW•G, to the extent they deliver content through Web browsers, its subcontractor and service provider, Microsoft, generally endeavors to ensure compatibility with the latest versions of the most popular browsers including Internet Explorer, Firefox, Chrome and Safari. As of the date of Offeror's Proposal, each of these are supported. However, CDW•G respectfully declines to commit to any requirement that would constrain Microsoft's ability to evolve its services to meet market needs. Over the 10 year term of the Master Agreement, it is likely that browser technology will change, and Microsoft will make decisions (independent of contractual commitments) as to how it will support future versions of these browsers.

Requirement

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.

Response

When requested, CDW•G, in conjunction with Microsoft, will coordinate cooperative meetings pertaining to information storage.

For ease of obtaining this information, customers can refer to Microsoft's most Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance document. As an example, we have included the most recent version of this document with our Business Profile.

Requirement

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

Response

When CDW•G provides services, we utilize our Customer Success Project Methodology. This methodology is focused on aligning the project with the business strategy of our customers, and ensuring that the project provides the expected value to the business. We have built project governance throughout our methodology. Having governance activities occur within the Monitor and Control ensure that the project remains in alignment, even as project scope or business strategy changes. The chart below outlines our overall framework, and governance is covered in the following tasks:

In the Initiate Phase

- Perform contract / SOW review
- Conduct internal project kick off

In the Planning Phase

- Scope Confirmation
- Stakeholder analysis
- Determine project success criteria
- Define roles and responsibilities
- Develop Project Plan
 - Communication Plan
 - Stakeholder Management Plan

In Monitor and Control Activities

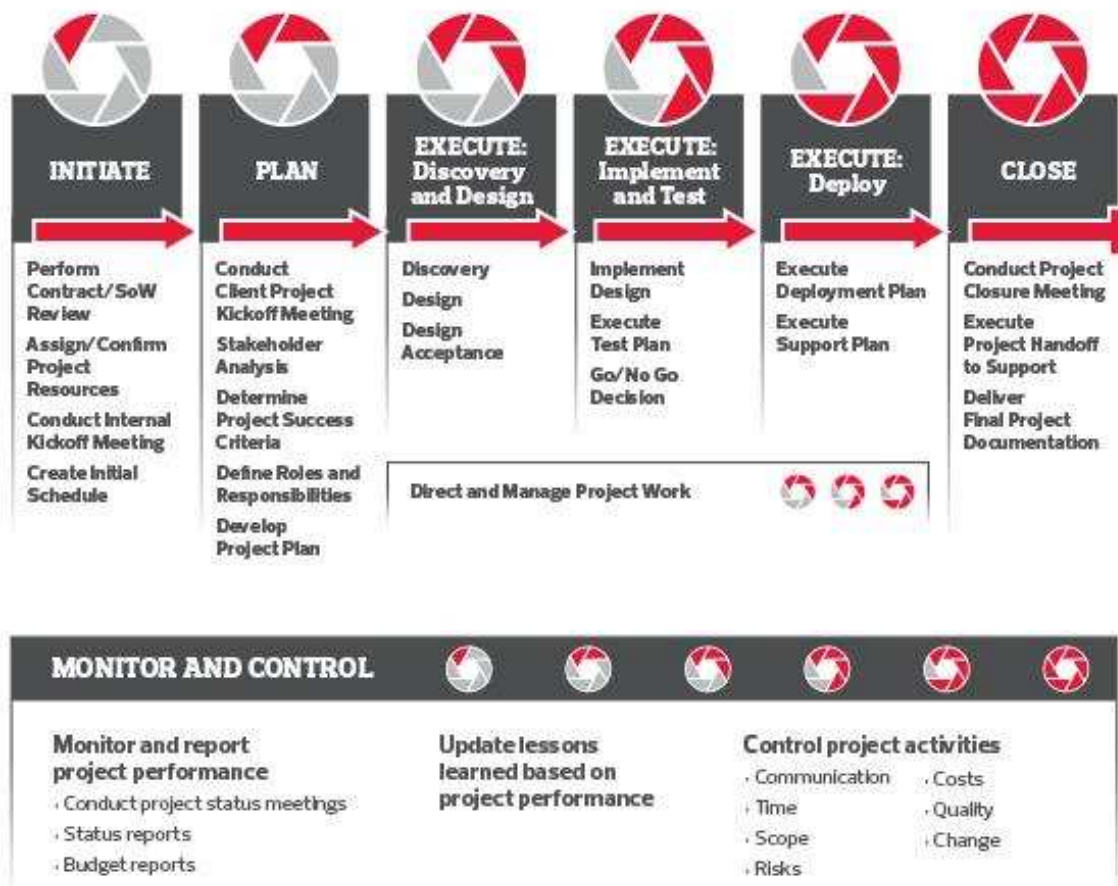
- Monitor and report project performance
- Control project communications
- Control project quality
- Update lessons learned

In the Execute Phase

- Direct and Manage Project Work
 - Stakeholder Engagement
 - Quality

In the Close Phase

- Conduct Project Closure Meeting
 - Review Lessons Learned



CDW•G, provides on an individual, per-customer basis the timelines and project plans for development, testing, and implementation of a specific cloud solution.

8.4 Customer Service (E)

Requirement

8.4.1 Describe in detail how you ensure excellent customer service is provided to Purchasing Entities. Include:

- Quality assurance measures;
- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA). Please note that the terms and conditions of this RFP and all exhibits take precedence over any conflicting terms and conditions in the SLA.

Response

We provide all applicable SLAs as an attachment to the Minimum Mandatory response. This document includes an SLA Summary for each of the proposed solutions. Details for each service and qualifications describing the SLA are also included.

Requirement

8.4.2 Specify your ability to comply with the following customer service requirements:

- a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.
- b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.
- c. Customer Service Representative will respond to inquiries within one business day.
- d. You must provide design services for the applicable categories.
- e. You must provide Installation Services for the applicable categories.

Response

Microsoft Azure Premier Support

Support is available in markets where Microsoft Azure is offered. Some specific services may not be covered in all regions immediately after General Availability (GA).

- Unlimited 24x7 technical support
- Unlimited 24x7 billing & subscription support
- Escalation management
- Minimum response times.

Another option for customers to consider is Azure Rapid Response in addition to the Azure Premier Support Contract.

Business applications and platforms which leverage public cloud services require around the clock availability, lightning fast user response, and resiliency to handle unforeseen events. Microsoft Cloud includes these capabilities today and now so can your support team.

By nominating a customer and being selected, adding Azure Rapid Response to a Microsoft Premier Support agreement your customers can receive 15 minute response time, access to a dedicated team of trusted advisors, and access to proactive services.

8.5 Security of Information (E)

Microsoft believes that our customers should control their own data whether stored on their premises or in a cloud service. Accordingly, they will not disclose Customer Data to a third party (including law enforcement, other government entities or civil litigants) except as our customers direct them or as required by law.

Should a third party contact Microsoft with a demand for Customer Data, they will attempt to redirect the third party to request it directly from our customers. As part of that, they may provide customers' basic contact information to the third party. Microsoft requires a court order or warrant before we will consider disclosing content to law enforcement. If compelled to disclose Customer Data to a third party, they will promptly notify the customer and provide a copy of the demand to them, unless legally prohibited from doing so.

Microsoft also publishes a Law Enforcement Requests Report that provides insight into the scope and number of requests. To learn more about how Microsoft responds to requests for

Customer Data, read the Responding to government legal demands for Customer Data blog post from Microsoft's General Counsel.

Microsoft will use your customer data only to provide the services they have agreed upon, and for purposes that are compatible with providing those services. They do not share your data with our advertiser-supported services, nor do they mine it for marketing or advertising.

Requirement

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.

Response

Microsoft has leveraged its decades-long experience building enterprise software and running some of the world's largest online services to create a robust set of security technologies and practices. These help ensure that Azure infrastructure is resilient to attack, safeguards user access to the Azure environment, and helps keep customer data secure through encrypted communications as well as threat management and mitigation practices, including regular penetration testing.

Managing and controlling identity and user access to your environments, data, and applications by federating user identities to Azure Active Directory and enabling multi-factor authentication for more secure sign-in.

Encrypting communications and operation processes. For data in transit, Azure uses industry-standard transport protocols between user devices and Microsoft datacenters, and within datacenters themselves. For data at rest, Azure offers a wide range of encryption capabilities up to AES-256, giving you the flexibility to choose the solution that best meets your needs.

Securing networks. Azure provides the infrastructure necessary to securely connect virtual machines to one another and to connect on-premises datacenters with Azure VMs. Azure blocks unauthorized traffic to and within Microsoft datacenters, using a variety of technologies. Azure Virtual Network extends your on-premises network to the cloud through site-to-site VPN.

Managing threats. To protect against online threats, Azure offers Microsoft Antimalware for cloud services and virtual machines. Microsoft also employs intrusion detection, denial-of-service (DDoS) attack prevention, regular penetration testing, and data analytics and machine learning tools to help mitigate threats to the Azure platform.

CDW•G has our own policies to safeguard from an order processing and billing perspective. CDW complies with PCI DSS, HIPAA, and Sarbanes-Oxley. For example, encryption is in place to protect Confidential/Restricted information.

Our record retention schedule is enforced based on record type, not by customer. Once the retention period has been reached, the data is deleted from our systems. Should CDW be awarded this RFP, CDW will provide additional details regarding the scope of the disposal processes.

Requirement

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

Response

As mentioned above, we comply with PCI DSS, HIPAA, and Sarbanes-Oxley.

As it pertains to Microsoft Online Services sold under the Master Agreement, CDW•G and its subcontractor, Microsoft, will comply with all applicable laws (including but not limited to privacy and security related laws) applicable to IT service providers. For clarity, however, CDW•G and Microsoft do not agree to comply with laws written to apply solely to governments and their government functions (or to companies and their industry functions). For example, some laws pertaining to notification of security incidents apply to our government customers (not to IT Service Providers), so CDW•G and Microsoft do not agree to comply with those (but we believe our contractual commitments for Security Incident reporting are sufficient to help customers comply with their own laws).

Requirement

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.

Response

Governed by Microsoft privacy policies and the Microsoft Privacy Standard, privacy is built into the infrastructure of Microsoft cloud services.

The Microsoft Privacy Standard is a cornerstone of the privacy program at Microsoft. This authoritative document describes the Microsoft privacy program, including the business processes we follow to achieve privacy compliance. It also delineates the general privacy rules and requirements for developing and deploying Microsoft products and services, including those in the Microsoft Cloud. It sets rules to help Microsoft keep your customer data secure, and handle and store the data you entrust to them in a way that helps protect its privacy.

Microsoft Security Development Lifecycle (SDL). Privacy requirements are defined and integrated early in the SDL, a software development process that helps developers build Microsoft Cloud services and features that are more secure and that help address data

protection and privacy requirements. As part of this process, the SDL is designed to support effective privacy reviews of each release of a Microsoft Cloud service.

Microsoft contractual commitments back their privacy best practices

Online Services Terms. These are the contractual commitments Microsoft makes to their enterprise cloud customers to secure and protect both the use and the disclosure of customer data. We have included a copy of these terms as an attachment to this response. Microsoft will use customer data only to provide the services agreed upon, and for purposes (such as troubleshooting and protection against malware) compatible with providing those services. They do not use customer data or derive information from it for advertising.

Furthermore, they will not disclose customer data hosted in the Microsoft Cloud to government agencies except as you direct or where required by law. If they do receive a request, they will promptly notify you unless legally prohibited from doing so.

ISO/IEC 27018:2014. Microsoft was the first major cloud provider to adopt this first international code of practice for cloud privacy. ISO/IEC 27018 was developed to establish a uniform international approach to protecting the privacy of personal data stored in the cloud by data processors. As part of the certification process for ISO/IEC 27001, accredited certification bodies independently verified that in-scope Microsoft enterprise cloud services have incorporated ISO/IEC 27018 controls. These controls include a prohibition on the use of customer data for advertising and marketing purposes without the customer's express consent. Microsoft contractually commits to complying with ISO/IEC 27018.

EU Model Clauses. EU data protection law regulates the transfer of EU customer personal data to countries outside the European Union. Microsoft offers customers the EU Standard Contractual Clauses that provide specific contractual guarantees around transfers of personal data for in-scope services. Europe's privacy regulators have determined that the contractual privacy protections that the Microsoft Cloud delivers to its enterprise cloud customers meet current EU standards for international transfers of data. Microsoft was the first cloud provider to receive this recognition.

8.6 Privacy and Security (E)

Requirement

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.

Response

Microsoft enterprise cloud services are independently validated through certifications and attestations, as well as third-party audits. In-scope services within the Microsoft Cloud meet key international and industry-specific compliance standards, such as ISO/IEC 27001 and

ISO/IEC 27018, FedRAMP, and SOC 1 and SOC 2. They also meet regional and country-specific standards and contractual commitments, including the EU Model Clauses, UK G-Cloud, Singapore MTCS, and Australia CCSL (IRAP). In addition, rigorous third-party audits, such as by the British Standards Institution and Deloitte, validate the adherence of our cloud services to the strict requirements these standards mandate. For more information, please refer to the Windows Azure Security Privacy Compliance document included with our Minimum Mandatory response.

Requirement

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.

Response

The National Institute of Standards and Technology (NIST) 800-53 controls is the standard, and FedRAMP is the program that certifies that a cloud service provider (CSP) meets that standard. FedRAMP, ISO/IEC 27001 and ISO/IEC 27018, SOC 1 and SOC2.

Microsoft Azure and Microsoft Azure Government have earned a Provisional Authority to Operate (P-ATO) from the FedRAMP Joint Authorization Board; Microsoft Dynamics CRM Online Government has received an Agency ATO from HUD; and Microsoft Office 365 U.S. Government has received an Agency ATO from DHHS.

The US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11 lists requirements for the security of electronic records of companies that sell food and drugs manufactured or consumed in the United States

The Defense Information Systems Agency (DISA) Cloud Service Support has granted a DISA Impact Level 2 Provisional Authorization (PA) to Microsoft Azure, Microsoft Azure Government, Microsoft Office 365 MT, and Microsoft Office 365 U.S. Government, based on their FedRAMP authorizations.

Microsoft contractual commitments, customers that are subject to FERPA can use Microsoft Azure, Microsoft Dynamics CRM Online, and Microsoft Office 365 and comply with FERPA.

NIST publishes a list of vendors and their cryptographic modules validated for FIPS 140-2. Rather than validate individual components and products, Microsoft certifies the underlying cryptographic modules used in Microsoft products, including Microsoft enterprise cloud services.

Microsoft engaged outside assessors to validate that Microsoft Azure and Microsoft Office 365 meet the FISC Version 8 requirements. Microsoft enterprise cloud services offer customers a HIPAA Business Associate Agreement (BAA) that stipulates adherence to HIPAA's security and privacy provisions. Microsoft Azure and Microsoft Office 365 were

among the first cloud services to achieve this certification for the storage and processing of unclassified (DLM) data.

Microsoft Azure Government and Microsoft Office 365 U.S. Government cloud services provide a contractual commitment that they have the appropriate controls in place, and the security capabilities necessary for customers to meet the substantive requirements of IRS 1075.

The ISO/IEC 27001 certificate validates that Microsoft enterprise cloud services have implemented the internationally recognized information security controls defined in this standard, including guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization.

Microsoft was the first cloud provider to adhere to the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

Azure complies with Payment Card Industry (PCI) Data Security Standards (DSS) Level 1 version 3.0, the global certification standard for organizations that accept most payment cards and store, process, or transmit cardholder data.

A Voluntary Product Accessibility Template, or VPAT, is a standardized form developed by the Information Technology Industry Council to document whether a product meets key regulations of Section 508, an amendment to the Rehabilitation Act of 1973. Microsoft offers detailed VPATs for many of its core cloud services, describing the accessibility features of those services.

Service Organization Controls (SOC) are a series of accounting standards that measure the control of financial information for a service organization. Azure's SOC 1 and SOC 2 Type 2 audit reports attest to the effectiveness of the design and operation of its security controls. Other country-specific standards and contractual commitments, including the EU Model Clauses, UK G-Cloud, Singapore MTCS, and Australia CCSL (IRAP).

Microsoft has a responsibility to process our customers' information in a trustworthy manner, many of you have a responsibility to comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data. To give you the foundation to achieve that compliance, Microsoft takes a two-pronged approach to help ensure that compliance controls are current and that we build and maintain a dynamic compliance framework.

Additional Clarifying Statement from Microsoft: NIST Special Publication 800-145 is a set of definitions, general characteristic and recommendations for cloud services, but was not intended by NIST as a control set or framework for "Compliance." Not all cloud services can be expected to conform to all of the characteristics outlined therein.

Offeror, on behalf of its subcontractor, Microsoft, will agree that, during the term of a Purchasing Entity's subscription for its "Government Community Cloud Services" (as defined in Microsoft's terms and conditions), those services will be operated in accordance with a written data security policy and control framework that is consistent with the requirements of NIST 800-53 Revision 4, or successor standards and guidelines (if any), established to support Federal Risk and Authorization Management Program (FedRAMP) accreditation at a Moderate Impact level. Microsoft intends for Government Community Cloud Services to support FedRAMP Authority to Operate (ATO), and Microsoft will use commercially reasonable efforts to obtain an ATO from a Federal agency, and to maintain such ATO through continuous monitoring processes and by conducting regular FedRAMP audits.

For information about Microsoft's compliance and adherence to other standards, such as CJIS, IRS 1075, HIPAA, FERPA, ISO/IEC 27001 and 27018, SOC1 and 2, and others, please refer to their Trust Center Website. Please note that some of these standards apply only to certain services (e.g. CJIS applies only our Government Community Cloud services) and that some of them require special Amendments and/or Agreements (e.g. CJIS requires that a State's CJIS Systems Agency must execute a special agreement with Microsoft, before Microsoft will provide an FBI CJIS Addendum for use in each such state). Microsoft welcomes the opportunity to discuss this in more detail during negotiation.

Requirement

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.

Response

Azure Government delivers a trusted foundation on which customers can design, build and manage their own secure cloud applications and infrastructure. It also provides transparent accountability to allow customers and their agents to track administration of applications and infrastructure, by themselves and by Microsoft. Below are the key security control areas that Microsoft has invested in.

Infrastructure Protection

Azure infrastructure includes hardware, software, administrative and operations staff, and physical data centers. Azure addresses security risks 24X7 across its infrastructure with continuous intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools that help identify and mitigate threats. With Azure, customers can reduce the need to invest in these capabilities on their own and benefit from economies of scale in Microsoft datacenter infrastructure.

Perimeter 	Buildings 	Computer room 
• 24x7 security staff • Facility setback requirements • Barriers • Fencing	• Alarms • Security operations center • Seismic bracing • East/Central locations: U.S. Gov. Iowa & U.S. Gov. Virginia	• Two-factor access control: Biometric & card readers • Camera • Days of backup power

- **24 hour monitored physical security** - Datacenters are physically constructed, managed, and monitored to shelter data and services from unauthorized access as well as environmental threats.
- **Monitoring and logging** - Security is monitored with the aid of centralized monitoring, correlation, and analysis systems that manage the large amount of information generated by devices within the environment and providing timely alerts.
- **Patching** - Integrated deployment systems manage the distribution and installation of security patches. Customers can apply similar patch management processes for Virtual Machines deployed in Azure.
- **Antivirus/Antimalware protection** - Microsoft Antimalware is built-in to Cloud Services and can be enabled for Virtual Machines to help identify and remove viruses, spyware and other malicious software and provide real time protection. Customers can also run antimalware solutions from partners on their Virtual Machines.
- **Intrusion detection and DDoS** - Intrusion detection and prevention systems, denial of service attack prevention, regular penetration testing, and forensic tools help identify and mitigate threats from both outside and inside of Azure.
- **Penetration testing** - Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of a customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their applications hosted in Azure

Network Protection

Azure networking provides the infrastructure necessary to securely connect VMs to one another and to connect on-premises data centers with Azure VMs. Azure blocks unauthorized traffic to and within Microsoft data centers using a variety of technologies such as firewalls, partitioned Local Area Networks, and physical separation of back-end servers from public-facing interfaces.

- **Network isolation.** Network isolation prevents unwanted tenant-to-tenant communications, and access controls block unauthorized users from the network. Virtual machines do not receive inbound traffic from the Internet unless customers configure them to do so.

Virtual networking. A customer can assign multiple deployments within a subscription to a virtual network and allow those deployments to communicate with each other using private IP addresses. Each virtual network is isolated from other virtual networks.

- **Encrypting communications.** Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on premise data centers. Encryption can be configured to protect administrator access to virtual machines through remote desktop sessions and remote Windows PowerShell. Access to the Azure Management Portal is encrypted by default using HTTPS.

Identity and Access

Azure Active Directory is a comprehensive identity and access management solution in the cloud. It combines core directory services, advanced identity governance, security, and application access management. Azure Active Directory makes it easy for developers to build policy-based identity management into their applications.

- **Access monitoring and logging** - Security reports are used to monitor access patterns and to proactively identify and mitigate potential threats. Microsoft administrative operations, including system access, are logged to provide an audit trail if unauthorized or accidental changes are made. Customers can turn on additional access monitoring functionality in Azure and use third-party monitoring tools to detect additional threats. Customers can request reports from Microsoft that provide information about user access to their environments.
- **Strong authentication** - Azure Multi-Factor Authentication reduces organizational risk and helps enable regulatory compliance by providing an extra layer of authentication, in addition to a user's account credentials, to secure employee, customer, and partner access. Azure Multi-Factor Authentication can be used for both on-premises and cloud applications.
- **Role-based access control** - Multiple tools in Azure support authorization based on their role, simplifying access control across defined groups of users.

Data Protection

Both technological safeguards, such as encrypted communications, and operation processes help keep Customer Data secure. Customers have the flexibility to implement additional encryption and manage their own keys.

- **Data in transit.** Azure uses industry-standard transport protocols such as SSL and TLS between user devices and Microsoft data centers, and within data centers themselves. With virtual networks, customers can use industry standard IPsec protocol to encrypt traffic between their corporate VPN gateway and Azure. Customers can enable encryption for traffic between their own VMs and end users.
- **Data at rest.** Customers are responsible for ensuring that data stored in Azure is encrypted in accordance with their standards. Azure offers a wide range of encryption capabilities up to AES-256, giving customers the flexibility to choose the solution that best meets their needs. Options include .NET cryptographic services, Windows Server public key infrastructure (PKI) components, Active Directory Rights Management Services (AD RMS), and BitLocker for data import/export scenarios.
- **Data segregation.** Azure is a multi-tenant service, meaning that multiple customers' deployments and virtual machines are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.
- **Data destruction.** When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before reuse, as well physical destruction of decommissioned hardware.
- For additional security information refer to the security best practices or Azure Security Insights documents on Microsoft's Azure Trust Center.

Requirement

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.)

Response

Microsoft has made major investments in cloud security in the following areas.

Design and operational security

Microsoft Cloud security begins with a trustworthy technology foundation. Microsoft designs its software for security from the ground up and helps ensure that the cloud infrastructure is resilient to attack. They use an "assume breach" stance as a security strategy, and their global incident-response team works around the clock to mitigate the effects of any attacks against the Microsoft Cloud. These practices are backed by centers of excellence that fight digital crime, respond to security incidents and vulnerabilities in Microsoft software, and combat malware.

Encryption

Technological safeguards, such as encrypted communications and operational processes, enhance the security of our customers' data. For data in transit, the Microsoft Cloud uses industry-standard encrypted transport protocols between user devices and Microsoft datacenters, and within datacenters themselves. For data at rest, the Microsoft Cloud offers a wide range of encryption capabilities up to AES-256, giving you the flexibility to choose the solution that best meets your needs.

Identity and Access Management

Azure Active Directory is a comprehensive identity and access management cloud solution that helps secure access to your data and on-premises and cloud applications, and simplifies the management of users and groups. It combines core directory services, advanced identity governance, security, and application access management, and is a key component of Microsoft Cloud services, including Microsoft Azure, Office 365, Microsoft Dynamics CRM Online, and Intune, as well as thousands of third-party SaaS apps. Azure Active Directory also makes it easy for developers to build policy-based identity management into their applications.

Security Development Lifecycle

Microsoft recognizes that focusing on security as a core component in the software development process can reduce the risk of costly issues, improve the security and privacy of infrastructure and applications, and protect data in the Microsoft Cloud. The SDL is composed of proven security practices that consist of multiple phases in which core software assurance activities are defined. Microsoft Azure uses multiple safeguards to protect customer and enterprise data. These security practices and technologies include:

- **Identity and access management.** Azure Active Directory helps ensure that only authorized users can access your environments, data, and applications, and provides multi-factor authentication for highly secure sign-in.
- **Encryption.** Azure uses industry-standard protocols to encrypt data as it travels between devices and Microsoft datacenters, and crosses within datacenters
- **Secure networks.** Azure infrastructure relies on security practices and technologies to connect virtual machines to each other and to on-premises datacenters, while blocking unauthorized traffic. Azure Virtual Networks extend your on-premises network to the cloud via a site-to-site virtual private network (VPN). You can also use ExpressRoute to create a cross-premises connection when needing to use the Internet.
- **Threat management.** Microsoft Antimalware protects Azure services and virtual machines. Microsoft also uses intrusion detection, denial-of-service (DDoS) attack

prevention, penetration testing, data analytics, and machine learning to constantly strengthen its defense and reduce risks.

- **Compliance.** We comply with both international and industry-specific compliance standards and participate in rigorous third-party audits, which verify our security controls.

Customers maintain full ownership and control over their own data. Microsoft is a leader in providing transparency about our privacy practices—one reason they have adopted the world's first code of practice for cloud privacy, ISO/IEC 27018.

Requirement

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.

Response

Where Azure data is physically stored is very important to most customers. If the organization is restricted by any government regulations or internal company policies about data storage and location, this needs to be transparent. Many times there are restrictions about data export and Government Regulatory Compliance (GRC) for some data sets. This information needs to be understood before deploying any applications or services.

Within each datacenter, the racks of equipment are built to be fault tolerant with respect to networking, physical host servers, storage, and power. The physical host servers are placed in high availability units called a cluster. The cluster configurations are spread across multiple server racks.

A single rack is referred to as a Fault Domain (FD), and it can be viewed as a vertical partitioning of the hardware. The fault domain is considered the lowest common denominator within the datacenter for fault tolerance. Microsoft Azure can lose a complete rack, and the hosted services can continue unaffected.

A second partition within the datacenter is called the Upgrade Domain (UD) and it can be viewed as a set of horizontal stripes passing through the vertical racks of fault domains. Upgrade domains are used to deploy updates (security patches) within Azure without affecting the availability of the running services within the Azure fabric. The following diagram shows a high-level relationship between fault domains and update domains in the Azure datacenters.

Microsoft has been a leader in creating robust online solutions that protect the privacy of our customers for twenty years. Today, we operate more than 200 cloud and online services that serve hundreds of millions of customers across the globe. Our enterprise cloud services, such as Office 365 and Windows Azure, serve millions of end users whose companies entrust their mission-critical data to Microsoft.

Our experience has enabled us to develop industry-leading business practices, privacy policies, compliance programs, and security measures that we apply across our cloud computing ecosystem. Driven by a commitment to empower organizations to control the collection, use, and distribution of their data, our time-tested approach to privacy provides a solid foundation for addressing customer privacy requirements and enabling greater trust in cloud computing.

Requirement

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.

Response

Microsoft Azure complies with both international and industry-specific compliance standards and participates in rigorous third-party audits, which verify our security controls.

Customers maintain full ownership and control over their own data. We are a leader in providing transparency about our privacy practices—one reason we have adopted the world's first code of practice for cloud privacy, ISO/IEC 27018.

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements.

Customers can request compliance reports for all logging and security controls through Microsoft's Office online support page. For more information, we include attachment "Microsoft Azure Security and Audit Log Management.

Requirement

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

Response

You can enable or disable the following kinds of logs:

- **Detailed Error Logging.** Detailed error information for HTTP status codes that indicate a failure (status code 400 or greater). This may contain information that can help determine why the server returned the error code.
- **Failed Request Tracing.** Detailed information on failed requests, including a trace of the IIS components used to process the request and the time taken in each component. This can be useful if you are attempting to increase site performance or isolate what is causing a specific HTTP error to be returned.
- **Web Server Logging.** Information about HTTP transactions using the W3C extended log file format. This is useful when determining overall site metrics such as

the number of requests handled or how many requests are from a specific IP address.

We include the Azure Security and Audit Log Management attachment as an additional resource for information regarding this request.

Requirement

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.

Response

Because each virtual network is run as an overlay, only virtual machines and services that are part of the same network can access each other. Services outside the virtual network have no way to identify or connect to services hosted within virtual networks. This provides an added layer of isolation to your services.

You can join virtual machines in Azure to your domain running on-premises. You can access and leverage all on-premises investments for monitoring and identity for your services hosted in Azure.

Azure Resource Management RBAC roles have support for Azure Service Management API (Classic) resources using the following RBAC roles:

- Classic Network Contributor
- Classic Storage Contributor
- Classic Virtual Machine Contributor

Using these RBAC roles, it is possible to assign limited access to classic resources in the ARM Azure portal. The access is restricted to the abilities in the ARM portal for management of the resources.

RBAC is supported on classic Compute, Storage, and Networking objects. Compute includes IaaS VMs and PaaS Web/Worker roles. Networking includes vNets and subnets (NSGs are currently not supported). Storage includes storage accounts. Only classic resources in these three roles are supported.

Azure Resource Manager provides the ability to restrict operations on resources through resource management locks. Locks are policies which enforce a lock level at a particular scope. The scope can be a subscription, resource group or resource.

The lock level identifies the type of enforcement for the policy, which presently has two values—CanNotDelete and ReadOnly. CanNotDelete means authorized users can still read and modify resources, but they can't delete any of the restricted resources. ReadOnly means authorized users can only read from the resource, but they can't modify or delete any of the restricted resources

Locks can be applied using ARM templates, ARM REST API, or ARM Azure PowerShell. To create or delete management locks, you must have access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions. Of the built-in roles, only Owner and User Access Administrator are granted those actions.

Every request made to an Azure Storage account must be authenticated, unless it is an anonymous request against a public container or its blobs. There are two ways to authenticate a request against the storage accounts:

- Use the shared key or shared key lite authentication schemes for the Blob, Queue, Table, and File services.
- Create a shared access signature. A shared access signature includes the credentials required for authentication and the address of the resource being accessed. Because the shared access signature includes all data needed for authentication, it can be used to grant access to a Blob, Queue, or Table service, and it can be distributed separately from any code.

Security Incident Notification

If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

"Microsoft Online Services Terms February 2016.doc"

Electronic Notices

Microsoft may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

Incident Response Process

- Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.
- For each security breach that is a Security Incident, notification by Microsoft (as described in the “Security Incident Notification” section above) will be made without unreasonable delay and, in any event, within 30 calendar days.
- Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.

Service Monitoring

Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.

Microsoft Security Development Lifecycle (SDL)

Microsoft Security Development Lifecycle is supported in Azure, part of that development processes is notification. Azure has security controls in place to implement threat mitigation and also to assist customers mitigate potential threats in their environments. Microsoft maintains continuous monitoring across servers, networks, and applications to detect threats and prevent exploits. Automated alerts notify administrators of anomalous behaviors, allowing them to take corrective action on both internal and external threats.

Our Microsoft Operations Centers (MOCs) are globally distributed and work around the clock in a “follow-the-sun” model to ensure our cloud services are persistently available. Each MOC is staffed with a team of incident management professionals and collectively they are responsible for monitoring service health, process automation, infrastructure operations, event and crisis management, and communications across the business. They are responsible for more than five hundred service components and monitor the servers and devices for the services we provide. Most critically, this is the team that identifies and resolves service incidents and outages when things go wrong.

In an environment with so many services, not all incidents are the same. Over half of all incidents are handled through automation and 90 percent of all incidents are handled at first touch. The most severe issues are resolved by a highly trained and qualified crisis management team, working on technical resolution, escalations, and communications to the impacted business groups.

Requirement

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.

Response

Operational Security Assurance (OSA) is an important process that Microsoft uses to make its networks more resilient to attack and increase the security of its cloud-based services. OSA helps Microsoft achieve this increased resilience and security by extending the foundation of Microsoft cloud-based services to protect against Internet-based security threats and by incorporating best practices and methodology to continuously update services to improve security and resolve incidents as quickly as possible.

The Security Development Lifecycle (SDL) is a software development process that helps developers build more secure software and address security compliance requirements while reducing development cost.

It is important for customers to realize the scale of engineering that is placed into the Microsoft Azure strategy. The designs are not for a single datacenter or a few dozen datacenters so the zoning must be completed at a Hyper-Scale level.

Hyper-scale

With more than 100 datacenters worldwide, we have datacenters located in every region, connected by one of the largest cloud networks in the world. There are only a few cloud providers who are individually enterprise grade, hybrid, or hyper-scale, but Microsoft's cloud is the only one that offers all three.

The distributed and virtual networks in Azure help ensure that each customer's private network traffic is logically isolated from traffic belonging to other customers. A customer subscription can contain multiple isolated private networks (and include firewall, load-balancing, and network address translation):

- Deployment network: Each deployment is isolated from other deployments at the network level. Multiple VMs within a deployment are allowed to communicate with each other through private IP addresses.
- Virtual network: Each virtual network is isolated from other virtual networks. Multiple deployments (inside the same subscription) can be placed on the same VNET, and allowed to communicate through private IP addresses.

By default, Virtual Machines inside the private network do not receive inbound traffic from outside of the deployment. The administrator defines an input endpoint that specifies which ports on which VMs should receive inbound traffic initiated from outside a deployment's isolated network—enabling traffic from the Internet and other deployments or customers inside Azure. Microsoft Azure uses multiple safeguards to protect customer and enterprise data. These security practices and technologies include:

- **Identity and access management.** Azure Active Directory helps ensure that only authorized users can access your environments, data, and applications, and provides multi-factor authentication for highly secure sign-in.
- **Encryption.** Azure uses industry-standard protocols to encrypt data as it travels between devices and Microsoft datacenters, and crosses within datacenters
- **Secure networks.** Azure infrastructure relies on security practices and technologies to connect virtual machines to each other and to on-premises datacenters, while blocking unauthorized traffic. Azure Virtual Networks extend your on-premises network to the cloud via a site-to-site virtual private network (VPN). You can also use ExpressRoute to create a cross-premises connection when needing to use the Internet.
- **Threat management.** Microsoft Antimalware protects Azure services and virtual machines. Microsoft also uses intrusion detection, denial-of-service (DDoS) attack prevention, penetration testing, data analytics, and machine learning to constantly strengthen its defense and reduce risks.
- **Compliance.** We comply with both international and industry-specific compliance standards and participate in rigorous third-party audits, which verify our security controls.

Physical zoning and Virtual Zoning of HOST systems is supported through Microsoft Azures extensive use of Software-Defined Networks which spans across datacenter from edge computing not to the interval fiber backbones.

- **Physical Access to Facilities.** Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.
- **Physical Access to Components.** Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain.
- **Protection from Disruptions.** Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.
- **Component Disposal.** Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.

With software enablement for restricting access, security is critical to provide customer data and privacy. Microsoft goes beyond ISO and NIST standards to ensure physical and virtually safe environments. As an example in the Azure infrastructure there is Separation of CPU's Storage, SQL Services that supports greater Zoning and Security requirements.

Software-Defined Networks (In Support of Zoning)

To improve flexibility and accelerate the adoption of advanced technologies into our network, we have broadly adopted a software-defined networking (SDN). SDN provides the ability to dynamically modify our network using automated management tools to move data and resources to an area where it is best served. In an SDN environment, we are able to extract and separate the application, the control plane, and the transport of the data. This allows us to insert our own APIs to gain visibility of how the data flows and gain better control, and allows us to upgrade network performance outside of the hardware refresh cycle. Our large, geographically distributed footprint of datacenters and networks enables us to be located close to our customers to reduce network latency and allow for geo-redundant back-up and failover.

Requirement

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)

Response

Complication with attempting to use traditional network-based security controls exclusively is that most of these controls assume the IP address is a good proxy for machine or service identity.

IP addresses are a poor proxy for identity outside of a corporate LAN that is using static assignments, particularly in a globally scaled Internet service such as Azure where IP addresses change rapidly. This typically creates significant challenges for organizations that are overly reliant on network security measures and are using static IP addresses for server and service mapping.

Review the guidance in the Microsoft Azure Security section (specifically the Containment and Segmentation Strategy) for how to design complete security containment strategies that overcome the limitations of networking controls alone.

Virtual Appliances are third-party-based virtual machine solutions that can be selected from the Azure Gallery or Marketplace to provide services like network firewall, application firewall and proxy, load balancing, and logging.

As organizations move workloads to the cloud, they must address threats in new ways and shed legacy security practices that often have proven to be ineffective and burdensome. In some cases, extending to the cloud provides an opportunity to implement security controls and contain adversaries in ways that are more challenging to accomplish in existing on-premises environments. Although containment strategies are not new, the traditional network-centric approach has failed in several ways and needs to be updated.

This section defines the following terminology:

- **Containment strategy.** High-level strategic approach designed to limit the risk and scope of any given compromise
- **Segmentation strategy.** Component of the containment strategy that separates computing assets into security zones that reflect significantly different asset valuation, trust levels, and/or risk exposure profiles
- **Security zone.** Set of computing assets with a common asset valuation, trust level, and/or risk exposure profile.

The notions of containment and segmentation have been around for a long time in IT security, though the interpretations of how to implement them have varied in practice. This document starts with an assume breach mindset and calls for designing security controls to prevent propagation of breaches among enterprise assets. This requires architects and system designers to look at what a breached system or compromised account means to the environment so as to limit the impact of that breach, to make it detectable, and to enable the organization to respond. This assume breach approach complements the traditional perimeter approach focused on preventing breaches for a combined approach that results in a more resilient strategy.

While the challenges of providing security and privacy are evolving along with the cloud, the underlying principles haven't changed. We work to build secure systems that will help protect an individual's privacy and we adhere to clear, responsible privacy policies in our business practices—from software development through service delivery, operations, and support.

Microsoft's Online Services Security and Compliance team operates a comprehensive security program and control framework that is evaluated regularly by external parties. The ISO standard is the foundation of our program. While the ISO/IEC 27001:2013 certification standard includes about 150 security controls for our scope, we adhere to more than 800 security controls. We choose to exceed the standard to manage risks that are unique to a cloud infrastructure. In addition, our security program and capabilities are subject to a SSAE16/ISAE3402 review.

The FISMA certification and accreditation, ISO certification, and SSAE16 SOC 1, 2, and 3 Type I and Type II attestations demonstrate Microsoft's commitment to delivering a trustworthy cloud computing infrastructure.

Other audits and assessments that the Microsoft cloud infrastructure environment undergoes on a regular basis include: the Payment Card Industry Data Security Standard, Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), and Media Ratings Council for the integrity of advertising system data generation and processing.

Operational Security Assurance (OSA) is a framework that incorporates the knowledge gained through a variety of capabilities that are unique to Microsoft, including the Microsoft

Security Development Lifecycle (SDL), the Microsoft Security Response Center program, and deep awareness of the cybersecurity threat landscape.

One of the goals of OSA is to reduce threat identification and response times by ensuring that online services have effective attack detection capabilities and are capable of fielding a unified response team that can resolve incidents rapidly and at scale.

Another goal of OSA is to complement recognized standards such as NIST Special Publication 800-53 (the standard that underlies Federal Information Security Management Act [FISMA] certifications and ISO 27001.

Microsoft employs a Security Information Management process that aligns with ISO/IEC 18044 and NIST SP 800-61. Azure Anti-Malware is enabled by default on all infrastructure servers. You can optionally enable it within your own VMs. You have the option to deploy 3rd-party security solutions within your subscriptions, such as web application firewalls from Barracuda.

Microsoft's approach to penetration-testing includes "Red-Teaming", which involves Microsoft security professionals attacking (non-customer) live production systems in Azure to test defenses against real-world, advanced persistent threats.

Security and privacy are embedded in the Azure platform, using the Security Development Lifecycle (SDL), from initial planning through solution launch—as well as the upgrades we continue to make.

Thread modeling activities include the service design and enumerating STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) threats across all trust boundaries has proven an effective way to catch design errors early.

In the event that customer data is compromised, Microsoft will notify its customers. Azure has comprehensive, transparent policies that govern incident response from identification all the way through to lessons learned.

Requirement

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.

Response

Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Microsoft Personnel. Microsoft personnel will not process Customer Data without authorization from Customer. Microsoft personnel are obligated to maintain the security and

secrecy of any Customer Data as provided in the DPT and this obligation continues even after their engagements end.

Subcontractor Transfer. Microsoft may hire subcontractors to provide certain limited or ancillary services on its behalf. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Each Online Service has a website that lists subcontractors that are authorized to access Customer Data as well as the limited or ancillary services they provide. At least 14 days before authorizing any new subcontractor to access Customer Data, Microsoft will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent Customer invoices.

For more information on Microsoft's applicable security practices, please refer to the table on pages 11-12 of their Online Services Terms included with this response.

Requirement

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.

Response

Microsoft encrypts customer data at transit and at rest and provides a complaint platform to NIST standards. Industry and government regulations such as HIPAA and FedRAMP, and international standards such as ISO 27001, lay out specific safeguards through processes and policies. It is a shared responsibility between Microsoft Azure and its customers to implement sufficient mechanisms to meet those obligations. Specifically, Microsoft provides a compliant platform for services, applications, and data, while Azure customers must design and configure their cloud environment to ensure the confidentiality and integrity of their information assets.

There are multiple tools within Microsoft Azure to safeguard data according to your company's security and compliance needs. One of the keys to data protection in the cloud is

accounting for the possible states in which your data may occur, and what controls are available for that state. Specifically:

- **At Rest.** This includes all information storage objects, containers, and types that exist statically on physical media, be it magnetic or optical disk.
- **In Transit.** When data is being transferred between components, locations or programs, such as over the network, across a service bus (from on-premises to cloud and vice-versa, including hybrid connections such as ExpressRoute), or during an input/output process, it is thought of as being in-motion. Being in-transit does not necessarily mean a communications process with a component outside of your cloud service; it moves internally, also, such as between two virtual networks.
- **In Use or In Process.** Dynamic data usage could be a table kept in virtual memory, transactions in a message queue, or even encryption keys in the CPU cache. Information being acted upon in some way by the host or guest during a process, such as real-time database queries running in active memory (as opposed to a page file sent out to disk), could be in different security states depending on whether it is encrypted or decrypted, and the security context of the operator.

Further, there are two (2) fundamental types of data at rest:

- **Data in production.** There is data in some form of storage, e.g. Azure SQL Database, and compute processes that need to access that storage during production operations. In this case, encryption at rest is aimed at protecting the data in that storage (whereas the compute aspect deals with data in use).
- **Data not in production.** There is data in some form of storage, e.g. a Virtual Hard Disk (VHD), but that VHD is not in production use. For example, it may be part of an upgrade operation, but the VHD has not yet been loaded or mounted. Data encryption at rest is applicable here, but the compute aspect is not relevant for this scenario.

Specific to CDW•G, we understand that your privacy is an important part of the trust you place in us. This Policy explains how personal information of CDW customers is collected, used and disclosed by CDW LLC and its U.S. subsidiaries and affiliated companies ("CDW" or "We"). This privacy policy ("Policy") applies to the websites, online activities, and online services of CDW, including CDW.com and CDW's mobile applications (collectively, "our Sites") where we post our Policy. Except for CDW's own online activities on third-party websites and online services where we post our Policy, this Policy does not apply to, and CDW is not responsible for, any other data practices of third-party websites and online services or the practices of other third parties. To learn about third-party data practices, please visit their respective privacy policies. This Policy also does not apply to CDW websites or online services that display or link to different privacy statements.

Information Collected

We collect information about you in various ways, including the following.

Information You Provide

We collect information you provide us when you use our Sites. For example, we collect your name, email address, postal address, phone number, fax number, demographics, and other information you provide us online. We also collect credit card numbers and other forms of payment information if you purchase products and services through our Sites and certain third-party sites.

Information from Other Sources

We may also obtain information from other sources and combine that with information we collect on our Sites. As examples, we may obtain demographic data from third-party data providers to better market to you, and we may purchase or lease lists from list brokers to correct or supplement your data.

Information Automatically Collected

When you visit our Sites, some information about your visit is automatically collected by CDW's systems. For example, when you visit our Sites your computer's or mobile device's operating system, application software, Internet Protocol (IP) address, access times, browser type and language, peripherals, and the websites you visited before our Sites are logged automatically. We also collect information about your usage and activity on our Sites including information about your orders, purchases, and cart activity.

Cookies. We automatically collect information using "cookies." Cookies are small data files stored on your hard drive by a website. Among other things, cookies help us improve our Sites and your experience. As examples, we use cookies to see which areas and features are popular, to count visits to our Sites and to deliver personalized ads.

Web Beacons. We also collect information using Web beacons. Web beacons are electronic images used on our Sites and in our emails. We use Web beacons to deliver cookies, count visits, understand usage and campaign effectiveness and to tell if an email has been opened and acted upon.

Online Tracking by Third Parties

Other third parties may collect information about you through our Sites, including personally identifiable information about your online activities over time and across different websites when you use our Sites. Some third parties provide us with analytics services and automatically collect the type of information described above. Some third parties collect information on behalf of CDW and others for online advertising purposes described below.

Online Advertisements

We may use information collected using our own and third-party cookies and Web beacons on our Sites and in our emails to deliver CDW advertising displayed to you on third-party sites and social networking services. We use cookie information to know when you return to our Sites after visiting these third-party sites and services. We use this information and other information about you, including order and cart activity information, to try to understand your interests and show you relevant advertising and information about products and services offered by CDW and its partners. To learn about your choices regarding CDW's use of its own cookies to deliver personalized ads, [click here](#).

Certain third-party ad services may automatically collect information about your visits to this and other websites, your IP address, your ISP, and the browser you use to visit our Sites. They do this using their own cookies, Web beacons or other technologies. Information collected may be used, among other things, to deliver advertising relevant to your interests and to better understand the usage and visitation of our Sites and the other sites tracked by these third parties. This policy does not apply to, and we are not responsible for, third-party cookies or Web beacons, and we encourage you to check the privacy policies of advertisers and/or ad services to learn about their use of cookies and other technology. If you would like more information about the practices of many common ad services, [click here](#). If you would like more information about the practices of social networking services you use where CDW ads are displayed, please visit the respective privacy policies of those services.

Use Of Information We Collect

We use personal information collected online for purposes described in this Policy or disclosed to you on our Sites or in connection with our services. For example, we may use information that you provide or about you to:

- provide and deliver products and services you request;
- send you transaction related information, including confirmations, invoices, technical notices, product and services information, updates, security alerts, and support and administrative messages;
- respond to your comments and questions and provide customer service;
- operate and improve our Sites, products and services;
- facilitate the provision of software updates, product support, and other services related to our mobile applications;
- process and deliver contest entries and rewards;
- ask you to take part in research and surveys used to measure our performance and improve our products, services and customer experience;

- send you catalogs and communicate with you about new contests, promotions and rewards, upcoming events, and other news about products and services offered by CDW and our selected partners;
- link or combine with other personal information we get from third parties, to help understand your needs, customize our offerings to those needs and provide you with better service.

CDW may store and process personal information in the United States and other countries.

Sharing Of Personal Information

Ways we may share your personal information with third parties include the following:

- with your consent;
- with trusted third parties for their own marketing purposes in compliance with applicable laws and subject to their separate privacy policies;
- with third-party vendors, consultants and other service providers who work for us and need access to your information to do that work;
- with suppliers and distributors to CDW for their internal purposes including administrative purposes; to improve performance, products and services; and for purposes relating to proposed or completed transactions facilitated by CDW;
- to (i) comply with laws or to respond to lawful requests and legal process, (ii) to protect the rights and property of CDW, our agents, customers, and others including to enforce our agreements, policies and terms of use or (iii) in an emergency to protect the personal safety of CDW, its customers, or any person;
- in connection with or during negotiation of any merger, sale of company assets, financing or acquisition of all or a portion of our business to another company.
- We may also share aggregated or anonymized information in a form that does not directly identify you.

Security of Your Personal Information

CDW takes reasonable steps to help protect your personal information in an effort to prevent loss, misuse and unauthorized access, disclosure, alteration and destruction.

Your Information Choices And Changes

Email Choices

You may opt-out of receiving promotional emails from CDW by following the instructions in those emails. To manage your email or Catalog subscription, please visit our site. You may also make requests about your contact preferences and changes to your information by contacting your account manager. If you opt-out of promotional emails, we may still send

you non-promotional emails, such as emails about your accounts or our ongoing business relations.

Access and Change Requests

You may correct some personal and account information maintained in your E-Account through your E-Account. To request access to, or the correction or removal of any other information about you or content you post on our Sites, please contact your account manager. If you do not know your account manager, simply [click here](#) or call 866.782.4239. We reserve the right to decline requests unless required by applicable law.

Online Tracking Choices

When you visit our Site, we and others give you the following choices about use of mechanisms for tracking, including tracking of your online activities over time and across different websites and online services by third parties. Many Web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies from CDW and others. If you choose to remove cookies or reject cookies, this could affect certain features or services of our Site. You can choose to opt-out of use of cookies by certain third-party advertising networks to deliver ads tailored to your profile and preferences. To find out more and opt-out [click here](#) or visit our [About Cookies](#) page. If you delete your cookies, use a different browser, or buy a new computer, you will need to renew your opt-out choice. Please visit the respective privacy policies and/or review the privacy settings of the social networking services you use for the choices about CDW ads on those services. While we and others give you choices described in this Policy, there are many ways Web browser signals and other similar mechanisms can indicate your choice to disable tracking, and we may not be aware of or honor every mechanism.

Changes to This Policy

CDW may change this Policy from time to time. We include the date of the latest update on our [privacy policy site](#).

Requirement

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.

Response

Azure Billing APIs

The Azure Usage API and Azure RateCard API which provide customers and partners programmatic access to their Azure consumption and pricing details:

Azure Usage API

A REST API that customers and partners can use to get their usage data for an Azure subscription. As part of this new Billing API we now correlate the usage/costs by the resource tags you can now set on your Azure resources (for example: you could assign a tag “Department abc” or “Project X” to a VM or Database in order to better track spend on a resource and charge it back to an internal group within your company). To get more details, please read the MSDN page on the Usage API. Enterprise Agreement (EA) customers can also use this API to get a more granular view into their consumption data, and to complement what they get from the EA Billing CSV.

Azure RateCard API

A REST API that customers and partners can use to get the list of the available resources they can use, along with metadata and price information about them. These APIs could be made accessible to partners or other hosting providers using RBAC access. As an example of partner solutions in the Microsoft Azure marketing are Azure Billing partners (Cloudyn and Cloud Cruiser) have already integrated the new Billing APIs into their products:

- Cloudyn has integrated with Azure Billing APIs to provide IT financial management insights on cost optimization. You can read more about their integration experience in Microsoft Azure Billing APIs enable Cloudyn to Provide ITFM for Customers.
- Cloud Cruiser has integrated with the Azure RateCard API to provide an estimate of what it would cost the customer to run the same workloads on Azure. They are also working on integrating with the Azure Usage API to provide insights based on the Azure consumption. You can read more about their integration in Cloud Cruiser and Microsoft Azure Billing API Integration.

8.7 Migration and Redeployment Plan (E)

Requirement

8.7.1 Specify how you manage the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before you are 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.

Response

Data Retention

At all times during the term of Customer’s subscription, Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer’s subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer’s account and delete the Customer Data. The Online Service may not support retention or

extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data as described in this section.

Migration and redeployment is not part of solutions CDW•G is offering in this response.

As for return of data, Microsoft's approach is to provide self-service access to its customer's administrators to extract data upon termination. With regard to Office 365 Services, Microsoft Azure Core Services, Microsoft Dynamics CRM Online Services, and Microsoft Intune Online Services (as each is defined in the Microsoft Online Service Terms, or "OST"), Microsoft provides Customer administrators access to their Customer Data in the Online Services at all times during the term the subscription, and for at least 90 days thereafter (but for no more than 180 days). Where the modality of the Online Service is applicable and as described in the applicable service documentation and service descriptions at the time, Customer Data in the Online Services will be downloadable by the State in a common industry or published Microsoft format (e.g. MS Outlook PST files, MS Office document files in the then-current format, MS SQL Database files, CSV format files), during the term of each subscription and for a 90-day "limited functionality" period following expiration (as set forth in the Online Services Terms). For some Online Services service components (also variously described as workloads, services, or modules in Microsoft documentation) download is not possible (such as when the module provides for functionality to synchronize from primary copies of Customer Data held and maintained by the customer), or Customer is intended by the component design to prepare and develop or configure their own download modality (such as when Microsoft provides a platform for Customers own applications to be run as a cloud service).

Requirement

8.7.2 Specify how you intend 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.

Response

Import/Export Services

Customer's use of any Import/Export Service is conditioned upon its compliance with all instructions provided by Microsoft regarding the preparation, treatment and shipment of physical media containing its data ("storage media"). Customer is solely responsible for ensuring the storage media and data are provided in compliance with all laws and regulations. Microsoft has no duty with respect to the storage media and no liability for lost, damaged or destroyed storage media. All storage media shipped to Microsoft must be shipped DAP Microsoft DCS Data Center (INCOTERMS 2010). Storage media shipped to Customer will be shipped DAP Customer Dock (INCOTERMS 2010).

8.8 Service or Data Recovery (E)

Requirement

8.8.1 Specify 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. Experiences a business failure.
- d. Ability to recover and restore data within 4 business hours in the event of a severe outage.
- e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Response

Azure Backup can now back up your on-premises application workloads, including Microsoft SQL Server, Hyper-V virtual machines, Microsoft SharePoint, and Microsoft Exchange. You can back up your applications to a local disk or to Azure, allowing you to eliminate local tape libraries and leverage the unlimited storage capability of Azure.

You can also manage all your on-premises backups from a single user interface. Backup continues to support backups of your production IaaS virtual machines in Azure and to help protect your Windows client data and your shared files and folders. System Center Data Protection Manager is an option for on-premises, Azure, or Cloud Only backup and recovery.

Azure Site Recovery

ASRs enhanced VMware to Azure scenario is now Generally Available. This GA release, among other enhancements, is designed to help customers benefit from the following key functionality:

- Elimination of IaaS-based replication and orchestration components/appliance
- MSI-based unified setup of on-premises components, which significantly reduces the time and complexity to onboard to the scenario
- Non-disruptive disaster recovery testing with Test Failover
- ASR-integrated failback experience without vContinuum, with support for alternate location recovery, and original location recovery
- Disk-based replication from source machines, and driver installation without needing a source reboot
- Multi-VM Application and Crash-Consistent Replication for Windows and Linux
- Migration of protected machines from the in-market – Legacy – VMware to Azure scenario to the Enhanced VMware to Azure scenario
- Enterprise-grade enhancements such as support for FQDNs, custom ports, and installation paths
- Support for CentOS & RHEL 6.7, vCenter Server 6.0

Microsoft does not publish RPO or RTO.

Requirement

8.8.2 Explain and specify methodologies for the following backup and restore services:

- a. Method of data backups
- b. Method of server image backups
- c. Digital location of backup storage (secondary storage, tape, etc.)
- d. Alternate data center strategies for primary data centers within the continental United States.

Response

For its Government Community Cloud Services (as defined in Microsoft's service terms and conditions), or "GCC," Customer Content is stored at rest in the United States. In the cases of the GCC versions of Exchange Online, SharePoint Online, Skype for Business, and Dynamics CRM Online, the Customer Content is stored in encrypted format, whereas in the GCC version of Azure Core Services, customers are given the option to encrypt non-public Customer Content.

For the non-GCC (public) versions of the equivalent services, as well as for Microsoft Intune Online Services, certain types of Customer Content are stored at rest in the United States, if set up by the users in the United States. The terms and conditions governing where Customer Data will be stored may be found in the Microsoft Online Services Terms. Finally, for the non-GCC version of Azure Core Services, customers are given the choice of which of Microsoft's worldwide data centers to store and/or process data in.

For purposes of the above, "Customer Content" means the subset of Customer Data created by users. For Office 365 Services, Customer Content shall at least include Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), SharePoint Online site content and the files stored within that site, and Skype for Business Online archived conversations. For Microsoft Dynamics CRM Online Services, Customer Content shall be the entities of Customer Data managed by the Microsoft Dynamics CRM Online Services.

Please refer to the included Microsoft contract terms, which define Government Community Cloud services.

8.9 Data Protection (E)**Requirement**

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.

Response**Data at Rest**

Performed by the customer by encrypting the virtual hard disk (VHD) files. Microsoft and third-party mechanisms are used. Workloads (such as SQL Server) also support Transparent Data Encryption (TDE). Technologies that assist with this are:

- Key Vault
- SQL Server Transparent Data Encryption
- Azure Disk Encryption
- Third-party virtual machine volume encryption

Data in Transit

Performed by the customer by using transport encryption of traffic traversing exposed virtual machine network endpoints. Microsoft and third-party mechanisms are used. Actions performed by Microsoft include disk encryption using BitLocker Drive Encryption for bulk import/export operations and encrypting traffic between Azure datacenters. Technologies that assist with this are:

- HTTPS/REST API
- Azure endpoints
- Azure Import/Export service

Data Access

Performed by the customer by using native protections within the installed operating system to authenticate and authorize access to the virtual hard disk (VHD) data that is exposed through the operating system and published endpoints (for example, operating system file shares).

Requirement

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.

Response

Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Disclosure of Customer Data

Microsoft will not disclose Customer Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in the OST, or (3) as required by law.

Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to

redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third party request for Customer Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

Microsoft will not provide any third party: (a) direct, indirect, blanket or unfettered access to Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

Please refer to Microsoft's BAA for additional information. Microsoft's BAA is not negotiable, as they administer our HIPAA-based controls in a uniform manner. However, Microsoft believes that our BAA meets this requirement, such that no exception is required for this section 8.9.2.

Requirement

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.

Response

Customer Data will be used only to provide a Purchasing Entity the Online Services including purposes compatible with providing those services. CDW•G and Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, the Purchasing Entity retains all right, title and interest in and to Customer Data. Neither CDW•G nor Microsoft acquires any rights in Customer Data, other than the rights Customer grants to Offeror and its subcontractor, Microsoft, to provide the Online Services to Customer. This paragraph does not affect Microsoft's rights in software or Online Services Microsoft licenses to Purchasing Entity.

For DPT Services, CDW•G and Microsoft use data mining solely for the purposes of providing those cloud services, subject to the above-mentioned restrictions. Microsoft will not use data mining in the DPT Services for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security or service delivery analysis that is not explicitly authorized.

8.10 Service Level Agreements

Requirement

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.

Response

The Service Level Agreement for Microsoft Online Services is not negotiable, as it pertains to standardized multitenant cloud services, uniformly delivered to many thousands of customers and millions of users, and relies upon automated processes and standard operating procedures. Purchasing Entities benefit to the extent that Microsoft's SLA is competitive and of industry standard quality, and also benefit from the cost savings which standardized multitenant cloud services provide over the types of customized outsourcing services that would allow for such a negotiation.

Requirement

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.

Response

CDW•G includes Microsoft's most recent SLA as an attachment to our response to the Minimum Mandatory Requirements.

CDW•G is unable to negotiate Microsoft's SLA or submit to a Purchasing Entity's SLA requirements due to corporate policies surrounding the operational and security controls of its cloud service. For clarity, Microsoft's SLAs are administered in a consistent and in some cases automated way for all its customers, and may therefore not be customized. For any given cloud service, our SLA in effect as of the time a subscription order is first placed is locked and will not change during the term of a subscription order. Upon renewal of a Purchasing Entity's subscription order, Microsoft's then-current SLA will supersede the previous SLA. The Purchasing Entity's renewal of its subscription will constitute its written approval of the then-current (new) SLA.

Microsoft's historical practice has been to improve its SLAs over time, and they have never before adversely changed any SLA terms.

However, Microsoft's SLAs may not be customized for any customer, and they must reserve the right to change SLAs over time at our sole discretion, except to the extent one is locked for a subscription as noted above.

It is impossible for the provider of a standardized multi-tenant cloud service, provided uniformly to thousands of customers and millions of users, to design that service to meet each and every one of its customer's individual requirements. Microsoft, through CDW•G,

will transparently provide information about its Online Services to all Purchasing Entities so that they may judge for themselves whether the Online Services meet their needs. It will be up to each Purchasing Entity to determine whether Microsoft's SLA (and other services features, functions, and certifications) fit their needs.

Microsoft's SLA is not negotiable, as they administer their services (and apply credits when applicable) in a uniform manner.

8.11 Data Disposal (E)

Requirement

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

Response

Microsoft uses industry standard processes to delete Customer Data when it is no longer needed. Microsoft does not use customer data in non-production environments. In addition, Microsoft uses best practice procedures and a media wiping solution that is NIST 800-88 compliant. For hard drives that can't be wiped we use a destruction process that destroys it (i.e. shredding) and renders the recovery of information impossible (e.g., disintegrate, shred, pulverize, or incinerate). The appropriate means of disposal is determined by the asset type. Records of the destruction are retained. Microsoft Azure services utilize approved media storage and disposal management services. Paper documents are destroyed by approved means at the pre-determined end-of-life cycle.

Azure follows NIST 800-88 Guidelines on Media Sanitization, which address the principal concern of ensuring that data is not unintentionally released. These guidelines encompass both electronic and physical sanitization.

8.12 Performance Measures and Reporting (E)

Requirement

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.

Response

Guarantees vary by solution, please see included Microsoft's SLAs for guarantees for specific proposed solutions.

Requirement

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

Response

Guarantees vary by solution, please see included Microsoft's SLAs for guarantees for specific proposed solutions.

Requirement

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.

Response

The first point of contact for any CDW•G related support issues should be the participating entity's dedicated CDW•G Account Manager. Escalation point of contacts are listed on each participating entity's Account Center/Extranet Portal. Depending on the type of support needed, the CDW•G Account Manager will engage with appropriate resources. For example, if the support needed is pre-sales technical support, our dedicated Microsoft Azure technical specialists will be available to answer questions via coordination from the CDW•G Account Manager. If the support is more technical in nature, or considered Post Sales support, the participating entity's account manager will engage with the appropriate resources within Microsoft. If the support issue requires the participating entity to open a formal case/ticket with the Microsoft Azure Support team, the participating entity will need to submit the ticket/case directly with Microsoft.

Requirement

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

Response

Incident Response and Fix times are not part of Microsoft's SLA. To the extent that downtime results due to a service incident that is within the scope of Microsoft's standard SLA terms, those standard terms would provide a remedy based upon the amount of downtime. The same applies to downtime related to a disaster if the disaster is not otherwise excluded by Force Majeure or the terms and conditions of the SLA.

Requirement

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

Response

There are two types of Microsoft Azure platform events that can affect the availability of your virtual machines: planned maintenance and unplanned maintenance.

Planned maintenance events are periodic updates made by Microsoft to the underlying Azure platform to improve overall reliability, performance, and security of the platform infrastructure that your virtual machines run on. The majority of these updates are performed without any impact upon your virtual machines or cloud services. However, there are instances where these updates require a reboot of your virtual machine to apply the required updates to the platform infrastructure.

Unplanned maintenance events occur when the hardware or physical infrastructure underlying your virtual machine has faulted in some way. This may include local network failures, local disk failures, or other rack level failures. When such a failure is detected, the Azure platform will automatically migrate your virtual machine from the unhealthy physical machine hosting your virtual machine to a healthy physical machine. Such events are rare, but may also cause your virtual machine to reboot.

Microsoft Azure periodically performs updates across the globe to improve the reliability, performance, and security of the host infrastructure that underlies virtual machines. Many of these updates are performed without any impact to your virtual machines or Cloud Services, including memory-preserving updates.

However, some updates do require a reboot to your virtual machines to apply the required updates to the infrastructure. The virtual machines are shut down while we patch the infrastructure, and then the virtual machines are restarted.

Please note that there are two types of maintenance that can impact the availability of your virtual machines: planned and unplanned. This page describes how Microsoft Azure performs planned maintenance. For more information about unplanned maintenance, see [Understand planned versus unplanned maintenance](#).

There are two kinds of virtual machine configurations: multi-instance and single-instance. In a multi-instance configuration, similar virtual machines are placed in an availability set.

The multi-instance configuration provides redundancy across physical machines, power, and network, and it is recommended to ensure the availability of your application. All virtual machines in the availability set should serve the same purpose to your application. For more information about configuring your virtual machines for high availability, refer to [Manage the Availability of your Virtual Machines](#).

By contrast, a single-instance configuration is used for standalone virtual machines that are not placed in an availability set. These virtual machines do not qualify for the service level agreement (SLA), which requires that two or more virtual machines are deployed under the same availability set.

Follow best practices when you design your application for high availability. For more information about SLAs, refer to the "Cloud Services, Virtual Machines and Virtual Network" section of Service Level Agreements.

Requirement

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

Response

This Service Level Agreement for Microsoft Online Services (this "SLA") is a part of your Microsoft volume licensing agreement (the "Agreement"). Capitalized terms used but not defined in this SLA will have the meaning assigned to them in the Agreement. This SLA applies to the Microsoft Online Services listed herein (a "Service" or the "Services"), but does not apply to separately branded services made available with or connected to the Services or to any on-premises software that is part of any Service.

If Microsoft do not achieve and maintain the Service Levels for each Service as described in this SLA, then you may be eligible for a credit towards a portion of your monthly service fees. Microsoft will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, the version of this SLA that is current at the time of renewal will apply throughout your renewal term. We will provide at least 90 days' notice for adverse material changes to this SLA.

Requirement

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.

Response

Incident Response and Fix times are not part of Microsoft's SLA. To the extent that downtime results due to a service incident that is within the scope of Microsoft's standard SLA terms, those standard terms would provide a remedy based upon the amount of downtime. The same applies to downtime related to a disaster if the disaster is not otherwise excluded by Force Majeure or the terms and conditions of the SLA.

Requirement

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

Response

Customers have the ability to print historical, statistical and usage reports through the customer's Azure administrative portal.

Requirement

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

Response

Azure online services are managed by the customer through the customer's Administrative Console. When the customer's subscription is initiated, the customer can deploy on-demand at any time.

Requirement

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

Response

For Microsoft Azure Online Services managed through a customer's Administrative Console (e.g. storage, compute), all such services become available upon demand for use once the customer's subscription is initiated.

For other Microsoft Online Services that are sold as individual per-user licenses (e.g. Office 365 Services), once licenses have been obtained by a customer, deployment and reassignment of user accounts may be done in real time by a customer's administrator. However, the addition of new licenses requires that either (a) a purchase order is processed (which is not instantaneous); or (b) that a "License Reservation" is placed (subject to a contractual obligation to place an order). Some but not all) Microsoft cloud services may be reserved online, which results in licenses becoming available in a matter of minutes. Other cloud services require the processing of a paper form to reserve, and this may take several days. Microsoft will make a list available to Offeror of the SKUs that are eligible for License Reservation. Note that Microsoft cannot certify 1 hour provisioning time after License Reservation, but actual time frames should be close to this.

8.13 Cloud Security Alliance Questionnaires (E)

Requirement

Describe your level disclosure of compliance with CSA Star Registry for each Cloud solutions offered.

- a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.5
- b. Completion of Exhibits 1 and 2 to Attachment B
- c. Completion of a CSA STAR Attestation, Certification, or Assessment.
- D. Completion CSA STAR Continuous Monitoring.

Response

Office 365 was one of the first services to publish a self-assessment in the CSA's STAR; in 2012 Microsoft published a second self-assessment in the STAR, this time for Windows Azure. This means that customers or potential customers who are evaluating security practices for Office 365 or Windows Azure can use these self-assessments to understand whether these services fulfill the security, compliance, and risk management requirements that their organizations have. This information will help cloud customers save time, effort, and money in their efforts to understand how the security of these services is being managed. We have provided these documents, as well as Exhibit 1 to Attachment B as attachments to this response. The attachment titled "Standard Response to Request for Information Microsoft Azure Security, Privacy, and Compliance" contains the information requested in Exhibit 2 Attachment B.

8.14 Service Provisioning (E)

Requirement

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

Response

When a customer's subscription is initiated, the customer can order Azure services on-demand, any time, through the customer's Administrative Console.

Requirement

8.14.2 Describe in detail the standard lead-time for provisioning Services defined in section 8.4.2 of the RFP.

Response

For product recommendations, quotes, and other requests, Eligible Entities can reach out to their CDW•G Account Manager via phone, email, or fax. This information is displayed for each Eligible Entity on their CDW•G Account Center site, once logged in. Account Managers aim to respond to communication within 30 minutes to 2 business hours.

Whenever an Account Manager is out of the office, they designate a fellow coworker to assist their customers, so there is no gap in support. This designated backup will be

Account Manager that supports other Eligible Entities, to ensure they are knowledgeable of the contract requirements. As an extra point of redundancy, Eligible Entities can also reach out to our CDW•G general sales support team at the following: Telephone: 800.808.4239, online chat at cdwg.com, or email: cdwgsales@web.cdwg.com. Our Connecticut-based team staffing these lines of communication is available Monday through Friday 8AM-8:30 PM ET.

8.15 Back Up and Disaster Plan

Requirement

8.15.1 Ability to recover and restore data within 4 business hours in the event of a severe outage. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Response

Business Continuity Plans (BCPs) have been documented and published for critical Azure services, which provide roles and responsibilities and detailed procedures for recovery and reconstitution of systems to a known state per defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Plans are reviewed on an annual basis, at a minimum. The BCP team conducts testing of the business continuity and disaster recovery plans for critical services, per the defined testing schedule for different loss scenarios. Each loss scenario is tested at least annually. Issues identified during testing are resolved during the exercises and plans are updated accordingly.

Requirement

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

Response

Azure runs in geographically distributed Microsoft facilities, in some cases sharing space and utilities with other Microsoft Online Services (paired datacenters are located at least 300 miles apart in order to provide failover in the event of a large-scale regional disaster). Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel. Microsoft Azure also provides multiple mechanisms for customers to deploy fault-tolerance within their Azure subscription environment, including the configuration of failover clusters, geo-redundant storage, and load balancing.

Microsoft datacenter site selection is performed using a number of criteria, including mitigation of environmental risks. In areas where there exists a higher probability of earthquakes, seismic bracing of the facility is employed. Environmental controls have been implemented to protect systems inside the facility, including temperature and heating,

ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.

A single hardware failure is mitigated by a Fabric Controller which manages resource allocation, automatically failing-over to a different machine or cluster. Hardware management is transparent to the customer. Without additional configuration, data is protected by locally redundant storage, which maintains multiple replicas of data within a single region. If geo-replication for the virtual machine is configured, that geo-replication provides redundancy of data across regions to help ensure access to data in the event of a local disaster. Network infrastructure and components are similarly redundant, with N+1 links to regional TelCos, load balancers, and routing switch fabric.

Microsoft Azure employs sophisticated software-defined service instrumentation and monitoring that integrates at the component or server level, the datacenter edge, network backbone, Internet exchange sites, and at the real or simulated user level, providing visibility when a service disruption is occurring and pinpointing its cause. More importantly, Azure services teams continuously invest in developing greater application resiliency in software components so they will quickly recognize a disruption and gracefully fail over to a different set of servers or even a different datacenter, without interrupting the availability of the service. Azure datacenters have dedicated 24x7 uninterruptible power supply (UPS) and emergency power support, which may include generators. Regular maintenance and testing is conducted for both the UPS and generators, and datacenters have made arrangements for emergency fuel delivery. Datacenters also have a dedicated Facility Operations Center to monitor the following: Power systems, including critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.

Azure conducts a risk assessment to identify and assess continuity risks related to Microsoft Azure services. The Business Impact Analysis is carried out and impacts are assessed for critical services based on revenue and operations considerations. Business Impact Assessment, Dependency Analysis and Risk Assessments are performed /updated at least on an annual basis. Customers are responsible for performing impact analysis for their applications and design to meet their Recovery Time Objective (RTO) / Recovery Point Objective requirements.

CDW is also committed to business continuity and has a complete Business Continuity Program (BCP) for resuming our own business operations and for assisting our customers. This program is a part of our commitment to quality and is made up of five phases:

- 1.Prevention Phase: Ongoing preventative programs to help minimize threats
- 2.Response Phase: Initial response plans to identified manmade and natural threats

3. Resumption Phase: Recovery of critical business processes

4. Recovery Phase: Recovery of non-critical but important business processes

5. Restoration Phase: Rebuilding the infrastructure to former state of existence

Our BCP plans contain instructions, policies, and procedures for coworkers and management to follow during any business interruption. The BCP also includes an automated emergency communication system so we can contact appropriate team members simultaneously within minutes of an incident. Business interruptions addressed in the plans include:

- Bomb Threat
- Business Wrongdoing
- Chemical/Biological Attack
- Civil Disturbance
- Cyber Attack
- Explosion
- IT Infrastructure Failures
- Phone Outage - Server
- Internet - AS/400 1.LAN - WAN

2. WEB - Application

3. SQL Database

- Fire
- Hazardous Material Spill
- Major Vendor Loss
- Power Outage
- Snow/Ice Storm
- Tornado
- Workplace Violence

Our recovery strategies include: drop shipping, redundant IT systems, alternate office space, Sungard recovery services, and dual distribution centers. In an emergency situation, customers should be confident that CDW will work with you to ensure that systems are up and running as quickly as possible to minimize your downtime. Some other features of our BCP include:

- Redundant servers across data centers for all mission critical applications and web-site hosting (hot-site or load balancing redundancy)
- MS SQL and DB2 database replication for performance and availability
- Dual T3 internet connection
- Redundant phone capabilities
- Dual AC
- Dual UPS

- Diesel generators at both data centers
- Diesel generators at both distribution centers

The multiple redundancies built into our systems provide backup and switch over in the event of a disaster. As an example, our Herndon Virginia satellite office has redundant lines running out of opposite sides of the offices - providing continuous service of voice and data even if one side of the building should fail. We have two complete redundant data centers one in Vernon Hills, IL and one in North Las Vegas, NV. Our program is run through industry leading planning software, by Strohl called LDRPS (Living Disaster Recovery Programming System) and is backed up by written and laptop copies. This gives CDW the ability to maintain plans on an ongoing basis, make emergency notification through an automated process (NOTIFIND), and track response and recovery efforts as they occur (INCIDENT MANAGER). Data is stored offsite on a daily basis from our two primary data centers and it generally takes only one day to retrieve stored data. In addition, your CDW Storage Specialist can help your organization to maximize business continuity by moving data to another location or multiple locations. Services include virtualization, data replication, data migration, remote mirroring and snapshots. The disaster recovery program has been successful due to our commitment to quality systems and procedures that prevent disasters and our very knowledgeable staff that is dedicated to the continuous operation of our systems.

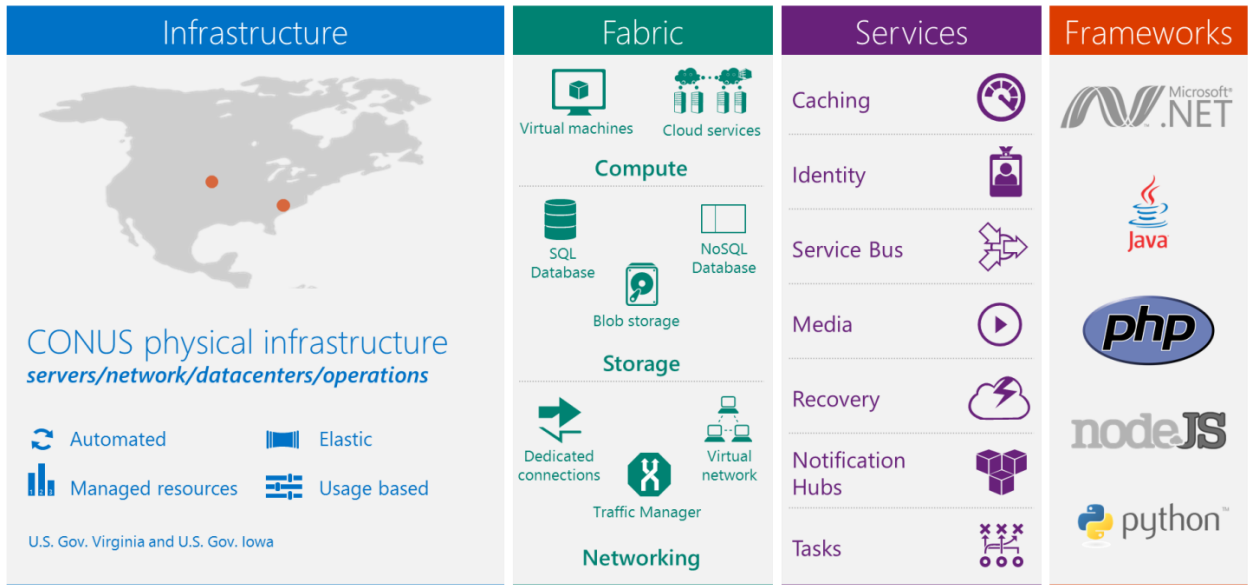
Requirement

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.

Response

Azure Government delivers a United States based cloud solution designed specifically to support strategic scenarios for U.S. government organizations including the Department of Defense, federal, state, and local governments, and their solution providers. It provides a comprehensive and open Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) for the U.S. government community including infrastructure, network, storage, data management and identity management delivered through secure and compliant hybrid cloud solution.

Azure Government core components include Compute, Storage, Networking, Identity and SQL database. Below is a diagram depicting the core capabilities that are delivered by Azure Government for IaaS and PaaS and will be discussed in detail below.



Azure Government was designed with the principles outlined below to help government organizations embrace cloud services. The key principles are:

- **Ease of Use** - Make it easy for developers, system administrators, and architects to build, migrate, deploy, and manage applications, and lets you accelerate provisioning of resources to minutes instead of days or months.
- **Open and Flexible** – Empower developers to choose the framework, tools, operating system and architecture to best meet their needs to build cloud solutions including .NET, Java, PHP and Node.js.
- **Secure and Compliant** – Ensure Azure Government is using Microsoft Azure’s world class security, compliance, and controls and is leveraging datacenters in the Continental U.S. (CONUS), screened U.S. personnel and policies to meet the higher level demands of US public sector customers.
- **Enterprise Ready**- Provides enormous scalability, reliability, and use of common management and identity tools that enables hybrid cloud solutions to quickly build, migrate, deploy, and manage, reliable and scalable applications using existing IT environments.

When organizations combine the core Azure Government services above with these principles, it enables them to implement relevant scenarios and capture the benefits of the cloud. In the Azure Government features section, we will break down the core components to help you understand the core services and then discuss some common workloads.

Azure Government provides a breadth of capabilities and services including infrastructure, fabric, services, and the frameworks that can be used to develop applications.

Its core capabilities include IaaS and PaaS which provides a rich set of compute, network infrastructure, storage, and identity management services. These provide government

organizations the flexibility to choose either approach to quickly build, test, deploy, and manage applications. All government customer data, applications, and hardware reside in the Continental United States (CONUS) and are operated by screened U.S. Citizens.

8.16 Solution Administration (E)

Requirement

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

Response

Managing identity is just as important in the public cloud as it is on premises. To help with this, Azure supports several different cloud identity technologies. They include these:

- You can run Windows Server Active Directory (commonly called just AD) in the cloud using virtual machines created with Azure Virtual machines. This approach makes sense when you're using Azure to extend your on-premises datacenter into the cloud.
- You can use Azure Active Directory to give your users single sign-on to Software as a Service (SaaS) applications. Microsoft's Office 365 uses this technology, for example, and applications running on Azure or other cloud platforms can also use it.

Applications running in the cloud or on-premises can use Azure Active Directory Access Control to let users log in using identities from Facebook, Google, Microsoft, and other identity providers. There are several options for connecting the domain controllers in the cloud with those running on premises:

- Make all of them part of a single Active Directory domain.
- Create separate AD domains on-premises and in the cloud that are part of the same forest.
- Create separate AD forests in the cloud and on-premises, then connect the forests using cross-forest trusts or Windows Server Active Directory Federation Services (AD FS), which can also run in virtual machines on Azure.

As SaaS applications become more and more common, they raise an obvious question: What kind of directory service should these cloud-based applications use? Microsoft's answer to that question is Azure Active Directory. There are two main options for using this directory service in the cloud:

- Individuals and organizations that use only SaaS applications can rely on Azure Active Directory as their sole directory service.
- Organizations that run Windows Server Active Directory can connect their on-premises directory to Azure Active Directory, then use it to give their users single sign-on to SaaS applications.

Administrators can federate on-premises AD or other directory stores with Azure AD. Microsoft recommends that organizations synch their on-premises directory information with SSO to ensure that users removed from on-premises directories are also removed from the Azure AD to maintain sufficient access controls. Deployment of a highly available Security Token Service (STS) (Active Directory Federation Services 2.0, or AD FS, for example) on-premises is required as this STS will become part of the authentication flow for every user login. Once federation is configured, all Azure AD users whose identities are based on the federated domain can use their existing corporate logon to authenticate to Azure AD services. Federation enables secure, token-based authentication and SSO across Azure applications.

Microsoft provides Multi-Factor Authentication for Azure administrators with a phone as the second factor; it also supports integration with third-party authentication solutions via on-premises STS integration.

Requirement

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

Response

Microsoft Antimalware offers customers the ability to install an antimalware agent for both PaaS roles and virtual machines. Based on System Center Endpoint Protection, this new feature brings proven on-premises security technology to the cloud.

We offer deep integration for Trend's Deep Security™ and SecureCloud™ products in the Azure platform. DeepSecurity is an Antivirus solution and SecureCloud is an encryption solution. DeepSecurity will be deployed inside of VMs using an extension model that Azure has already announced. Using the portal UI and PowerShell, customers can select to use DeepSecurity inside of new VMs that are being spun up, or existing VMs that are already deployed.

Symantec End Point Protection (SEP) is also supported on Azure. Through portal integration, customers have the ability to specify that they intend to use SEP within a VM. SEP can be installed on a brand new VM via the Azure Portal or can be installed on an existing VM using PowerShell.

For Office 365 Services, Microsoft Azure Core Services, Microsoft Dynamics CRM Online Services, and Microsoft Intune Online Services (as each is defined in the Microsoft Online Services Terms), Microsoft will implement and maintain all appropriate administrative, physical, technical and procedural safeguards in accordance with the terms and conditions of the Microsoft Online Services Terms, at all times during the term of the Master Agreement, to secure Customer Data from Security Incident, protect Customer Data and the applicable Online Services from hacks, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt a Purchasing Entity's

access to its Customer Data. Additionally, see the section of Microsoft's Service Level Agreement pertaining to anti-virus.

Requirement

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

Response

You can use Azure Active Directory's access and usage reports to gain visibility into the integrity and security of your organization's directory. With this information, a directory admin can better determine where possible security risks may lie so that they can adequately plan to mitigate those risks. In the Azure Management Portal, reports are categorized in the following ways:

- **Anomaly reports.** Contain sign in events that we found to be anomalous. Our goal is to make you aware of such activity and enable you to be able to make a determination about whether an event is suspicious.
- **Integrated Application reports.** Provides insights into how cloud applications are being used in your organization. Azure Active Directory offers integration with thousands of cloud applications.
- **Error reports.** Indicate errors that may occur when provisioning accounts to external applications.
- **User-specific reports.** Display device/sign in activity data for a specific user.
- **Activity logs.** Contain a record of all audited events within the last 24 hours, last 7 days, or last 30 days, as well as group activity changes, and password reset and registration activity.

Some advanced anomaly and resource usage reports are only available when you enable Azure Active Directory Premium. Advanced reports help you improve access security, respond to potential threats and get access to analytics on device access and application usage. Azure Active Directory Premium and Basic editions are available for customers in China using the worldwide instance of Azure Active Directory. Azure Active Directory Premium and Basic editions are not currently supported in the Microsoft Azure service operated by 21Vianet in China. The Azure Resource Usage and RateCard APIs are implemented as a Resource Provider, as part of the family of APIs exposed by the Azure Resource Manager.

Azure Resource Usage API

Customers and partners can use the Azure Resource Usage API to get their estimated Azure consumption data. The features include:

- **Azure Role-based Access Control.** Customers and partners can configure their access policies on the Azure Preview Portal or through Azure PowerShell cmdlets to

specify which users or applications can get access to the subscription's usage data. Callers must use standard Azure Active Directory tokens for authentication. The caller must also be added to either the Reader, Owner or Contributor role to get access to the usage data for a particular Azure subscription.

- **Hourly or Daily Aggregations.** Callers can specify whether they want their Azure usage data in hourly buckets or daily buckets. The default is daily.
- **Instance metadata provided (includes resource tags).** Instance-level details such as the fully qualified resource uri (/subscriptions/{subscription-id}/..), along with the resource group information and resource tags will be provided in the response. This will help customers deterministically and programmatically allocate usage by the tags, for use-cases like cross-charging.
- **Resource metadata provided.** Resource details such as the meter name, meter category, meter sub category, unit and region will also be passed in the response, to give the callers a better understanding of what was consumed. We are also working to align resource metadata terminology across the Azure portal, Azure usage CSV, EA billing CSV and other public-facing experiences, to enable customers to correlate data across experiences.
- **Usage for all offer types.** Usage data will be accessible for all offer types including Pay-as-you-go, MSDN, Monetary commitment, Monetary credit, and EA among others.

Requirement

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

Response

Role-Based Access Control (Commercial)

Azure Role-Based Access Control (RBAC) enables fine-grained access management for Azure. Using RBAC, you can segregate duties within your DevOps team and grant only the amount of access to users that they need to perform their jobs. Each Azure subscription is associated with one Azure Active Directory. Only users, groups, and applications from that directory can be granted access to manage resources in the Azure subscription, using the Azure portal, Azure Command-Line tools and Azure Management APIs.

Access is granted by assigning the appropriate RBAC role to users, groups, and applications, at the right scope. To grant access to the entire subscription, assign a role at the subscription scope. To grant access to a specific resource group within a subscription, assign a role at the resource group scope. You may assign roles at specific resources too, like websites, virtual machines and subnets, to grant access only to a resource.

Requirement

8.16.5 Ability to apply participating entity defined administration policies in managing solution

Response

Each subscription in Azure belongs to one and only one directory, each resource group belongs to one and only one subscription, and each resource belongs to one and only one resource group. Access that you grant at parent scopes is inherited at child scopes. If you grant reader role to an Azure AD group at the subscription scope, the members of that group will be able to view every resource group and every resource in the subscription. If you grant the contributor role to an application at the resource group scope, it will be able to manage resources of all types in that resource group but not other resource groups in the subscription.

The finer-grained authorization model (Azure RBAC) is supported only for management operations of the Azure resources in the Azure portal and Azure Resource Manager APIs. Not all data level operations for Azure resources can be authorized via RBAC. For instance, create/read/update/delete of Storage Accounts can be controlled via RBAC, but create/read/update/delete of blobs or tables within the Storage Account cannot yet be controlled via RBAC. Similarly, create/read/update/delete of a SQL DB can be controlled via RBAC but create/read/update/delete of SQL tables within the DB cannot yet be controlled via RBAC.

In Azure API Management, policies are a powerful capability of the system that allow the publisher to change the behavior of the API through configuration. Policies are a collection of Statements that are executed sequentially on the request or response of an API. Popular Statements include format conversion from XML to JSON and call rate limiting to restrict the amount of incoming calls from a developer. Many more policies are available out of the box.

8.17 Hosting and Provisioning (E)

Requirement

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

Response

Microsoft Azure Provisioning is an automated process that allows interaction from the Azure Portal or completely remote using Azure APIs, as a single example virtual machine in just a few minutes in the Azure portal. The normal steps take are the Planning for the deployment, selecting the VM image, creating the VM and then managing the virtual machine. The VM image can be from the images available from the gallery including Windows and Linux and the processes supports customized images from a customer's on-premise standard image template library. This process can be repeated one-at-a-time or automated with PowerShell to create hundreds of Virtual Machines at one time.

This example is for automating a VM however, all of the properties in Microsoft Azure can be automated using the same methods, through the portal or PowerShell. Other examples for automating include Cloud Storage, SQL Servers, Virtual Networks.

Requirement

8.17.2 Provide tool sets at minimum for:

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

Response

The Azure Portal provides the flexibility to create one or thousands of Virtual Machines (VMs). A single VM can be created and two or more VMs can be created and placed into an “availability set” so the uptime SLA is applied.

The Azure Portal and the underlining Azure APIs are used to extend or “scale” systems easily. Web Sites (PaaS) options in Azure are scaled by simply configurations in the Azure Portal to extend the Web Farm from 1 to 10 or more based on customized needs. For example the number of client connections, CPU utilization and other metrics could be configured once and the scale-out systems would deploy automatically, without administration interaction.

The Azure Portal supports Virtual Machines to be deployed into a previously created VM Farm. The VMs are created using automated processes and then configured either through the VM Operating System processes or automated by using scripting such as PowerShell.

Additionally custom virtual machines can be created using the same on-premises processes as today and they uploaded to the Azure Portal to include in the customer VM Library. Once the image is added to the library the automation processes for single VM deployment or joining to a VM Farm are exactly the same.

A custom virtual machine simply means a virtual machine that you create using the From Gallery option because it gives you more configuration choices than the Quick Create option. These choices include:

1. Connecting the virtual machine to a virtual network.
2. Installing the Azure Virtual Machine Agent and Azure Virtual Machine Extensions, such as for antimalware.
3. Adding the virtual machine to existing cloud services.
4. Adding the virtual machine to an existing Storage account.

5. Adding the virtual machine to an availability set.

Creating a custom image is completed on-premises and most customers have a processes for accomplishing this process. These steps are provided as one example of typical process steps.

Capture the Virtual Machine

1. In the Azure classic portal, Connect to the virtual machine. For instructions, see How to sign in to a virtual machine running Windows Server.
2. Open a Command Prompt window as an administrator.
3. Change the directory to %windir%\system32\sysprep, and then run sysprep.exe.
4. The System Preparation Tool dialog box appears. Do the following:
5. In System Cleanup Action, select Enter System Out-of-Box Experience (OOBE) and make sure that Generalize is checked. For more information about using Sysprep, see How to Use Sysprep: An Introduction.
6. In Shutdown Options, select Shutdown.
7. Sysprep shuts down the virtual machine, which changes the status of the virtual machine in the Azure classic portal to Stopped.
8. In the Azure classic portal, click Virtual Machines and select the virtual machine you want to capture.
9. On the command bar, click Capture
10. In Image Name, type a name for the new image.
11. Before you add a Windows Server image to your set of custom images, it must be generalized by running Sysprep as instructed in the previous steps. Click I have run Sysprep on the virtual machine to indicate you did that.
12. Click the check mark to capture the image. The new image is now available under Images.

With a cloud service previously created the addition of cloud storage can be automated using the Azure Portal or PowerShell. Azure Blob storage is a service that stores file data in the cloud. Blob storage can store any type of text or binary data, such as a document, media file, or application installer. Blob storage is sometimes referred to as object storage.

Azure Blob storage can be completely automated using .NET, Node.js, Java, C++, PHP, Ruby, Python, IOS, and Xamarin.

Common uses of Blob storage include:

- Serving images or documents directly to a browser

- Storing files for distributed access
- Streaming video and audio
- Performing secure backup and disaster recovery
- Storing data for analysis by an on-premises or Azure-hosted service
- Once the developer language is chose the steps are similar as this example
 - Create an Azure storage account
 - Generate a shared access signature
 - Create a new “Dev Language Choice” application
 - Use the share access signature to perform container operations
 - Rung the application

Monitoring cloud services are included in the Azure Portal and available from APIs in the Azure portal and on the individual VM available through the Operating System. You can monitor key performance metrics for your cloud services in the Azure classic portal. You can set the level of monitoring to minimal and verbose for each service role, and can customize the monitoring displays. Verbose monitoring data is stored in a storage account, which you can access outside the portal.

Monitoring displays in the Azure classic portal are highly configurable. You can choose the metrics you want to monitor in the metrics list on the Monitor page, and you can choose which metrics to plot in metrics charts on the Monitor page and the dashboard.

By default, minimal monitoring is provided for a new cloud service using performance counters gathered from the host operating system for the roles instances (virtual machines). The minimal metrics are limited to CPU Percentage, Data In, Data Out, Disk Read Throughput, and Disk Write Throughput. By configuring verbose monitoring, you can receive additional metrics based on performance data within the virtual machines (role instances). The verbose metrics enable closer analysis of issues that occur during application operations.

By default performance counter data from role instances is sampled and transferred from the role instance at 3-minute intervals. When you enable verbose monitoring, the raw performance counter data is aggregated for each role instance and across role instances for each role at intervals of 5 minutes, 1 hour, and 12 hours. The aggregated data is purged after 10 days.

After you enable verbose monitoring, the aggregated monitoring data is stored in tables in your storage account. To enable verbose monitoring for a role, you must configure a diagnostics connection string that links to the storage account. You can use different storage accounts for different roles.

Note that enabling verbose monitoring will increase your storage costs related to data storage, data transfer, and storage transactions. Minimal monitoring does not require a

storage account. The data for the metrics that are exposed at the minimal monitoring level are not stored in your storage account, even if you set the monitoring level to verbose. The steps are outlined below:

1. Configure monitoring for the cloud service (i.e. VM, SQL, Web Server)
2. Configure alert metrics from the metrics table
3. Customize the metrics chart
4. Enable verbose access monitoring data (outside the portal requires using the Azure Diagnostic APIs)
5. Configure alerts based on triggered metrics
6. Add metrics to the metric table for alerting as necessary

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

Requirement

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

Response

- a. CDW•G subcontractor, Microsoft, currently, as of the date of the Proposal, has a mechanism by which 30-day Trial subscriptions may be ordered for some, but not all, of the cloud services offered hereunder. Microsoft will provide additional information about this upon request of Lead State, Participating States, or any Purchasing Entity.
- b. It is possible for any Purchasing Entity to purchase a separate subscription for the purpose of establishing a second environment for test and/or staging purposes. Such separate Subscription would be at an additional cost, and additional contract paperwork may be required.

Requirement

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.

Response

As noted above:

- a. CDW•G subcontractor, Microsoft, currently, as of the date of the Proposal, has a mechanism by which 30-day Trial subscriptions may be ordered for some, but not all, of the cloud services offered hereunder. Microsoft will provide additional information about this upon request of Lead State, Participating States, or any Purchasing Entity.
- b. It is possible for any Purchasing Entity to purchase a separate subscription for the purpose of establishing a second environment for test and/or staging purposes. Such

separate Subscription would be at an additional cost, and additional contract paperwork may be required.

Requirement

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

Response

CDW•G's Account Executives are responsible for promoting the contract to end users; including trainings in the field with end users, presenting promotions and attend regional tech fairs to promote CDW•G and the contract. Additionally, they meet with the State and/or eligible for contract status and progress reports and assist in working out customer service issues in the field and the contract.

Our Licensing Specialists are training-focused as well. Examples of the types of training they are exposed to include Microsoft's weekly White Glove training. The weekly white glove is a weekly call Microsoft hosts to their LSP community. The Agenda typically consists of education around license program changes, licensing changes, and operational process announcements/changes. Additional examples of Microsoft training sessions include LSP Readiness webinars. These multi-session webinars include various levels of education from 100 level up to 400 level trainings on topics such as license program changes, quoting new offerings in EA and Select Plus agreements, in-depth licensing scenarios (product varies by session), Azure Partner university, and Azure in Government. Additionally, your licensing specialists consistently attend Microsoft's Partner network training, which include topics such as understanding O365 in Government, enterprise mobility training, partner enablement, and the Evolving EA. CDW•G Licensing Specialists participate in similar training programs for our other major software partners, as applicable and when available.

CDW•G often releases trainings to our customers as well, such as during the time of major product announcements by our software partners. These webinars articulate how licensing or solution changes may impact them and their IT environment.

8.19 Integration and Customization (E)

Requirement

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

Response

Microsoft Windows Azure is an internet-scale, high-availability cloud fabric operating on globally-distributed Microsoft data centers. Windows Azure and related tools support the

development and deployment of applications into a hosted environment that extends the on-premises data center.

On-demand self-service refers to the service provided by Microsoft Azure that enables the provision of resources on demand whenever required. In on-demand services can be enabled from the HTML Portal, using Azure API, using CLI for Mac, Linux, and Windows with Azure Service Management. Azure on-demand self-service resource sourcing programmatically is a prime feature allowing the user to scale the infrastructure.

Requirement

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

Response

Azure Government provides a breadth of capabilities and services including infrastructure, fabric, services, and the frameworks that can be used to develop applications.

Its core capabilities include IaaS and PaaS which provides a rich set of compute, network infrastructure, storage, and identity management services. These provide government organizations the flexibility to choose either approach to quickly build, test, deploy, and manage applications. All government customer data, applications, and hardware reside in the Continental United States (CONUS) and are operated by screened U.S. Citizens.

8.20 Marketing Plan (E)

Requirement

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

Response

CDW•G will utilize a number of proven activities to publicize and promote the NASPO ValuePoint cloud program. Our live touch approach includes a proactive outbound calling program, as well as both inside and field sales teams meeting directly with customers.

Our customers rely on their account manager as an expert resource; this includes leveraging contracts. Most often, when a customer purchases from a specific contract, it is because of a direct suggestion from their account manager. CDW•G's sales plan combines past CDW•G marketing successes with an innovative strategy to effectively capture net new business for the NASPO ValuePoint cloud contract.

CDW•G will promote the contract to our inside and field sales teams through mandatory sales training in close proximity of the program launch for each state. We will also focus on strategic field alignment to ensure our field teams align with Microsoft's field teams for NASPO white space account mapping.

We will leverage our reporting capabilities to determine which customers to target. After determining which customers to target, CDW•G can then sell them on the Microsoft solutions grow net-new business for NASPO. Through this method, NASPO ValuePoint and CDW•G will gain traction in these states faster than a supplier that does not have these existing relationships in place.

CDW•G will continue to follow all applicable requirements for use of the NASPO ValuePoint name and logo in marketing content.

8.21 Related Value-Added Services to Cloud Solutions

Requirement

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.

Response

CDW•G does not compete on price alone. As a vendor-agnostic solution provider, pre-sales recommendation support from our knowledgeable account teams and cloud specialists will always be an unparalleled differentiator when compared against our major competitors. We are a leading reseller for Microsoft, and our close partnerships mean we receive competitive price offers and early notifications regarding product changes, allowing the account managers serving NASPO ValuePoint members to keep their customers apprised of new product releases, version and price changes, and more in a timely manner. Our ability to serve NASPO ValuePoint customers participating in this contract is exponentially heightened by the myriad value-added benefits we provide **at no cost**. Specific to the solution proposed, we offer our Microsoft Azure White Glove Service.

Microsoft Azure White Glove Service

The service helps orient you to the capabilities in Azure that can be leveraged in a full production environment. CDW has experienced Azure Specialists to assist in helping you decide which components of Azure would help you accomplish your goals. Through the White Glove Service the Azure Specialists will assist in:

- Azure portal onboarding and tenant set up
- Azure Enterprise Portal Orientation
- Azure Management Portal Orientation
- Azure Infrastructure Orientation
- Azure Active Directory Orientation
- Azure Storage Orientation
- Planning for next steps

Benefits

- CDW's White Glove Service ensures a rapid onboarding process to make sure that you will be able to take full advantage of Microsoft Azure.
- You will gain knowledge and insight on the best use of Azure according to your business goals and requirements.
- Our Azure Specialists will share a number of best practices and techniques that we have developed through our experiences to ensure you get the most out of Azure and avoid common pitfalls.
- You will learn how to leverage Azure to deploy a test and development environment with little to no capital investment.
- You will learn how other customers are using Azure to cut costs while enjoying the benefits of a more agile IT environment

Effort Required

The Azure White Glove Service is 2 hours in length and done remotely in collaboration with your IT staff. Knowledge transfer is a critical component of this service and participation from all sponsors is strongly encouraged.

Additional Value Added Services

Additional Value Added Services include, but are not limited to, the following:

NO COST Value-Added Services for NASPO ValuePoint		
Benefit	Cost	Description
Solution Consultation Services	FREE	<i>Savings: over \$250/hour</i> Inside Solution Architects (ISAs)—technology and product experts—vet complex solutions, arrange product demos, webinars, and information documentation
Solution Design Services	FREE	<i>Savings: over \$300/hour</i> Field and inside engineers available for onsite access to customer environments, conduct assessment, provide technology-needs analysis
Threat Check	FREE	<i>Savings: \$3,000-5,000 per assessment</i> Passively monitors networks for unknown malware, alerts customers to active and installed malware, provide customized plan for remediation
Partner Assisted Grant Help	FREE	AMs assist with learning about available resources for segment-specific grant-finding processes
eProcurement Integration Services	FREE	Dedicated team integrating customer ePro systems for punch-out, PO delivery, eInvoicing, quote retrieval, order, and more
K-12 Consulting	FREE	<i>Savings: over \$250/hour</i> Former educators and educational technologists work as strategists to guide schools through high-access implementation and develop long-term adoption success plans
Digital Age Teaching and Learning Webinars	FREE	<i>Savings: over \$125 per attendee</i> CDW-G's Education Strategy Team conducts

NO COST Value-Added Services for NASPO ValuePoint		
Benefit	Cost	Description
		series of three one-hour webinars on latest technology trends in education
Track and Communicate CDW•G Software Webinars	FREE	CDW•G advertises to all contract holders and end users for webinars pertinent to COTS software on NASPO ValuePoint contract
Technical Trainings	FREE	<i>Includes two (2) trainings per calendar year</i> WebEx trainings specific to this contract, scheduled 60 days in advance on pertinent software (approx.. 30+ hours of CDW•G backend planning/work for each session0
CDW•G Blog	FREE	All interested parties under the contract will receive our Solutions Blog: blog.cdw.com ; internal engineers and SMEs write to relevant IT topics
Partner-Funded Programs	FREE	Leverage CDW•G relationship with key OEMs to get business development funds for projects users are potentially unable to fund independently
Marketing & Social Media	FREE	CDW•G collaboratively creates marketing materials and events with each participating state to promote adoption of contract
Technology Roadmapping Sessions	FREE	<i>Valued at \$1,000, one per year</i> Held by request with key software publishers and state customers, proctored by CDW•G sales teams

Other **free** benefits include access to CDW-badged product specialists, dedicated contract expert resources, Media Library access, and *free eligibility for state customers* interested in the Microsoft Rapid Deployment and Technology Adopter programs. Each participating state's specific account team offers additional value-added benefits, in terms of personnel and expertise, at no cost to the customer. These personnel include software licensing specialists, licensing account executives, pre-sale system engineers, software manufacturer representatives, and dedicated renewals specialists, program managers, account managers, and account executives.

8.22 Supporting Infrastructure (E)

Requirement

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

Response

The infrastructure requirements are going to vary widely based upon which service the purchasing entity wants, number of users, and, in some cases, intended use. Part of the value that CDW•G offers is pre-sales support. This will include discussing each entity's current infrastructure and what it needs to take full advantage of Microsoft 365 or Azure, based on their intended usage. Our pre-sales and account management teams are structured by customer type, so they'll already understand the most common uses for education, government, and not-for-profits, as well as the equipment the participating entity

currently has in place. Since we are named on many of the NVP IT contracts and also hold a number of other state-wide vehicles, CDW•G is well-positioned to not only offer custom advice on current infrastructure needs but also to fulfill those needs under contract.

Requirement

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

Response

For Microsoft cloud services, it will be the purchasing entity's responsibility to install any new infrastructure required at their site, and they will be the ones incurring costs. CDW•G has the resources to help with those installations, but as we understand it, networking, security, and end user devices, are not in scope of this contract. We would offer those services under other vehicles.

8.23 Alignment of Cloud Computing Reference Architecture

Requirement

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).

Response

NIST SP 800-145 defines Infrastructure-as-a-Service (IaaS) as *"The capability provided to the consumer is 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, and deployed applications; and possibly limited control of select networking components."*

Deploying an application and managing an IaaS environment provides the most flexibility that Azure has to offer. With any deployment choice, there will be pros and cons that must be considered. The greatest benefit of an IaaS implementation is that it offers the greatest amount of control from the operating system to manage access to the application.

IaaS is most like traditional IT delivery. Customers provision their own virtual machines, define their own networks, and allocate their own virtual hard disks. IaaS shifts the burden of operating datacenters, virtualization hosts, and hypervisors. In addition, the business continuity and disaster recovery infrastructure is shifted from the enterprise to the service provider.

NIST SP 800-145 defines Platform-as-a-Service (PaaS) as *"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported*

by the provider. 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 configuration settings for the application-hosting environment.”

With PaaS applications, many of the layers of management are removed and more flexibility is provided than an application running on IaaS instances. Specifically, there is no need to manage the operating system, including patching, which reduces some of the complexity of designing the deployment.

A significant benefit of deploying an application running in a PaaS environment is the ability to quickly and automatically scale up the application to meet the demand when traffic is high, and inversely scale down when the demand is less. Deploying an application in the PaaS model is very cost effective from a scalability and manageability perspective.

PaaS extends IaaS further by providing multitenant services that customers subscribe to. Platform services are a transformational computing model that can dramatically reduce the costs and increase the agility of delivering applications to end users internally and externally. PaaS users bring their own application code but leverage robust platforms, which they do not need to maintain.

NIST SP 800-145 defines Software-as-a-Service (SaaS) as *“The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either 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.”*

Choosing an Azure SaaS offering provides the least amount of responsibility on the customer’s side. At the same time, providing a lesser amount of flexibility in comparison with an IaaS or PaaS approach.

SaaS is the real promise of cloud computing. By integrating applications from one or multiple vendors, customers need to bring only their data and configurations. They can eliminate the costs of building and maintaining applications and platform services and still deliver the secure, robust solutions to the end users.

Many scenarios need to implement a blend of Azure offerings to meet the needs of their organization and application requirements. The following diagram highlights the main differences from a manageability perspective, when using public cloud SaaS, PaaS, IaaS and On-Premises implementations:



Attachment E

Microsoft NASPO ValuePoint Enterprise Agreement for Government Partners (GPEA)

Appendix A

Additional Use Rights and Restrictions

These Additional Use Rights and Restrictions shall apply to each Enterprise's use of Products and must be incorporated in each Government Contract.

1. General.

Right to use. Purchasing Entity may access and use In-Scope Services, and install and use a Client (if any) included with its Subscription, only as described in this agreement. All other rights are reserved.

Acceptable use. Purchasing Entity will use In-Scope Services only per the AUP. Purchasing Entity will not use In-Scope Services in any way that infringes a third party's patent, copyright, or trademark or misappropriates its trade secret. Purchasing Entity may not reverse engineer, decompile, workaround technical limits in, or disassemble In-Scope Services, except if applicable law permits despite this limit. Purchasing Entity may not rent, lease, lend, resell, transfer, or host In-Scope Services to or for third parties.

Compliance.

Purchasing Entity will comply with all laws and regulations applicable to its use of In-Scope Services.

In providing In-Scope Services, Contractor and Microsoft will comply with all laws and regulations (including applicable security breach notification law) that generally apply to IT service providers. Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry or government function that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Purchasing Entity will obtain any consents required: (1) to allow it to access, monitor, use, and disclose user data; and (2) for Contractor and Microsoft to provide the In-Scope Services. If Purchasing Entity is an educational institution, it will obtain any parental consent for end users' use of In-Scope Services as required by applicable law.

Customer Data. Customer Data is used only to provide Purchasing Entity In-Scope Services. This use may include troubleshooting to prevent, find and fix problems with those In-Scope Services' operation. It may also include improving features for finding and protecting against threats to users. Neither Contractor nor Microsoft will derive information from Customer Data for any advertising or other commercial purposes. As between the parties, the Purchasing Entity retains all right, title and interest in and to Customer Data. Neither Contractor nor Microsoft acquires rights in Customer Data, other than the rights Purchasing Entity grants to Microsoft through Contractor to provide the Online Services to Purchasing Entity. This paragraph does not affect Microsoft's rights in software or Online Services Contractor and Microsoft license to Purchasing Entity.

Contractor and Microsoft will enable Purchasing Entity to keep Customer Data in DPT Services separate from Microsoft's consumer services.

Customer Data will not be disclosed unless required by law or allowed by this agreement. Purchasing Entity's contact information may be provided so that a requestor can contact it. If law requires disclosure, Contractor and Microsoft will use commercially reasonable efforts to notify Purchasing Entity, if permitted.

Customer Data may be transferred to, and stored and processed in, any country Contractor or Microsoft maintain facilities, except when a tenant for DPT Services is provisioned in the United States, in which case Customer Content shall be processed and stored at rest in the Continental United States.

Security Incident Notification for DPT Services. Solely for DPT Services, the following terms and conditions apply:

If Microsoft becomes aware of any Security Incident (as defined herein), Microsoft will promptly (1) notify Purchasing Entity of the Security Incident; (2) investigate the Security Incident and provide Purchasing Entity with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Purchasing Entity's administrators by any means Microsoft selects, including via email. It is Purchasing Entity's sole responsibility to ensure Purchasing Entity's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Purchasing Entity must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any Security Incident related to an Online Service.

5-day Security Incident notification for Government Community Cloud Services. As an exception to the foregoing, notification of Security Incident solely pertaining to Government Community Cloud Services will be delivered within 5 days after Microsoft determines that a Security Incident has occurred, provided that Purchasing Entity must comply with the following requirements:

For each Online Service Tenant or Azure subscription, as applicable, as a condition of receiving notifications within 5 days, as set forth in the preceding paragraph, Purchasing Entity must register the following information by sending email to ols-notifications@microsoft.com, and must keep such information current at all times:

- 1) Purchasing Entity's Microsoft Online Direct Routing Domain (MODRD);
- 2) For one or more individual(s) to be contacted, each of whom must be registered as an administrator on the applicable Online Services, each of the following:
 - a. Name;
 - b. Title;
 - c. Email address registered as an administrator on the Online Services;
 - d. Email address not registered as a user on the Online Services;
- 3) Name of Purchasing Entity;
- 4) Enrollment number (provided by Contractor and assigned by Microsoft) to represent Purchasing Entity's Tenant or Azure Subscription, on Contractor's subcontract with Microsoft.

Microsoft expects to change the above process by which the Purchasing Entity for each tenant or subscription will be able to register their MODRD and other information for five-day Security Incident notification pursuant to these terms and conditions. In the event that a Purchasing Entity is notified by Microsoft, in the administrative console or otherwise, of revised instructions necessary to ensure five-day Security Incident notification, the Purchasing Entity must comply with such revised instructions.

Reimbursement of Security Incident Remediation Costs. To the extent that a Security Incident for a DPT Service results from Microsoft's failure to comply with its obligations under the Master Agreement (and, where applicable, Participating Addenda), and subject to the Limitation of Liability section in this Agreement, Microsoft will reimburse Purchasing Entities for reasonable out-of-pocket remediation costs incurred by such Purchasing Entities in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" are costs that (a) are customary, reasonable and expected to be paid by entities similar to Purchasing Entity, based on the nature and scope of the Security Incident, and (b) do not arise from or relate to Purchasing Entity's violation of (i) laws applicable to Purchasing Entity or (ii) Purchasing Entity's obligations to third parties, and (c) in no event include costs arising related to compliance with laws applicable to Purchasing Entity or its industry or government function that are not generally applicable to information technology services providers. Purchasing Entity must document all such expenditures and, upon Microsoft's request, those expenditures must be validated by an independent, internationally-recognized third party industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Microsoft under this paragraph will be characterized as

direct damages subject to the limitation on liability set forth in this Section, and not as special damages excluded under the “EXCLUSION OF CERTAIN DAMAGES” in the Limitation of Liability section.

Changes. In-Scope Services may be changed periodically. As such, Purchasing Entity’s use of them will be subject to a revised OST, then-current as of the date it renews its subscription. For In-Scope Services that include client software, Purchasing Entity may be required to run a client software upgrade on its devices after a change to maintain full functionality, in accordance with the terms and conditions of the OST.

Use rights. Use rights specific to each In-Scope Service are posted online at the link to the OST, which is hereby incorporated by reference into this agreement

2. Confidentiality and Security.

For DPT Services, Contractor and Microsoft will (a) implement and maintain all appropriate administrative, physical, technical, procedural safeguards and organizational measures, internal controls, and data security routines intended to protect Customer Data against accidental loss or change, unauthorized disclosure or access, unlawful destruction, hacks, introduction of viruses, disabling devices, malware, and other forms of malicious or inadvertent acts that can disrupt Purchasing Entity’s access to its Customer Data; and (b) not disclose Customer Data, except as required by law or expressly allowed. Neither party will make any public statement about this agreement’s terms without the other’s prior written consent.

3. Term, Termination, and Suspension.

Reserved

4. Limited warranty; disclaimer.

Contractor warrants that In-Scope Services will meet the SLA terms during the Subscription; Purchasing Entity’s only remedy for breach of warranty is stated in the SLA. Contractor provides no (and disclaims to the extent permitted by law any) other warranties, express, implied, or statutory, including warranties of merchantability or fitness for a particular purpose.

5. Indemnification.

Reserved

6. Limitation of Liability.

Reserved

7. Agreement mechanics

Purchasing Entity must send notice by regular mail, return receipt requested, to the address on the Portal (effective when delivered). Contractor or Microsoft may email notice to your account administrators (effective when sent). Purchasing Entity may not assign this agreement, or any right or duty under it. If part of this agreement is held unenforceable, the rest remains in force. Failure to enforce this agreement is not a waiver. The parties are independent contractors. This agreement does not create an agency, partnership, or joint venture. This agreement is governed by the laws applicable to Purchasing Entity, without regard to conflict of laws. This agreement (including the SLA and OST) and Contractor’s price sheet are the parties’ entire agreement on this subject and supersedes any concurrent or prior communications. Agreement terms that require performance, or apply to events that may occur, after termination or expiration will survive, including §5. In-Scope Service and any Client associated therewith are subject to U.S. export jurisdiction. Purchasing Entity must comply with the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end-use, and destination restrictions. For more information, see <http://www.microsoft.com/exporting/>. Microsoft delivers In-Scope Services, and the rights granted to us also apply to them.

8. Miscellaneous Microsoft Terms and Conditions

- A. Accessibility. Microsoft supports the government’s obligation to provide accessible technologies to its citizens with disabilities as required by Section 508 of the Rehabilitation Act of 1973, and its state law counterparts (including applicable California provisions). Microsoft encourages its customers (including Purchasing Entities under the Master Agreement and Participating Addenda)

to judiciously compare product accessibility performance. The Voluntary Product Accessibility Templates (“VPATs”) for the Microsoft technologies used in providing the online services can be found at Microsoft’s VPAT page. Further information regarding Microsoft’s commitment to accessibility can be found at www.microsoft.com/enable.

- B. DPT Services Information Security Policy. For each DPT Service, Microsoft follows a written data security policy (“Information Security Policy”) that complies with the control standards and frameworks shown in the table below.

DPT Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes*	Yes*
Microsoft Dynamics CRM Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Azure Core Services	Yes	Yes	Yes	Varies**	Varies**
Microsoft Intune Online Services	Yes	Yes	Yes	Yes	Yes

*Does not include Yammer Enterprise.

**Current scope is detailed in the audit report and summarized in the Microsoft Azure Trust Center.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate a standard or framework in the table above, unless it is no longer used in the industry and it is replaced with a successor (if any). Azure Government Services meet a separate set of control standards and frameworks, as detailed on the Microsoft Azure Trust Center.

Subject to non-disclosure obligations, Microsoft will make each Information Security Policy available to Purchasing Entity, along with other information reasonably requested by Purchasing Entity regarding Microsoft security practices and policies.

Purchasing Entity is solely responsible for reviewing each Information Security Policy and making an independent determination as to whether it meets Purchasing Entity’s requirements.

- C. Microsoft Audits of DPT Services. For each DPT Service, Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data), as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually for each DPT Service.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which will be Microsoft's Confidential Information. The Microsoft Audit Report will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor.

If Purchasing Entity requests, Microsoft will provide Purchasing Entity with each Microsoft Audit Report so that Purchasing Entity can verify Microsoft's compliance with the security obligations under the DPT. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

- D. HIPAA/HITECH Business Associate. If Purchasing Entity is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data, as those terms are defined in 45 CFR § 160.103, this agreement includes execution of the HIPAA Business Associate Agreement ("BAA"), the full text of which identifies the DPT Services to which it applies and is available at <http://aka.ms/BAA>. Purchasing Entity may opt out of the BAA by instructing Contractor to send the following information to Microsoft in a written notice (under the terms of the Contractor's subcontract with Microsoft):

- the full legal name of Purchasing Entity and any Affiliate that is opting out;
- the volume licensing agreement number to which the opt out applies.

- E. FedRAMP. During the term of a Purchasing Entity's subscription for Government Community Cloud Services, those services will be operated in accordance with a written data security policy and control framework that is consistent with the requirements of NIST 800-53 Revision 4, or successor standards and guidelines (if any), established to support Federal Risk and Authorization Management Program (FedRAMP) accreditation at a Moderate Impact level. Microsoft intends for Government Community Cloud Services to support FedRAMP Authority to Operate ("ATO"), and Microsoft will use commercially reasonable efforts to obtain an ATO from a Federal agency, and to maintain such ATO through continuous monitoring processes and by conducting regular FedRAMP audits.

- F. Background Checks. Microsoft performs the following background checks on all US personnel who have potential to access Customer Data. Adherence to this policy is one of the control procedures addressed by the Microsoft Audit Report per the section of the Microsoft Online Services Terms titled "Microsoft Audits of Online Services." Such Background Checks will be performed in accordance with the Fair Credit Reporting Act and will consist of Social Security Number trace, seven (7) year felony and misdemeanor criminal records check of federal, state, or local records (as applicable) for job related crimes, Office of Foreign Assets Control List (OFAC) check, Bureau of Industry and Security List (BIS) check and Office of Defense Trade Controls Debarred Persons List (DDTC) check.

Additionally, for States with which Microsoft has entered into a Microsoft CJIS Information Agreement and provided an FBI CJIS Addendum Certification to the applicable CJIS Systems Agency (CSA, e.g. the California Department of Justice), for its CJIS Covered Services (which are most of the Microsoft Government Community Cloud Services), Microsoft submits its personnel that have access to unencrypted Criminal Justice Information and other Customer Content (including both employees and subcontractors, where applicable) for FBI NCIC fingerprint background checks and adjudication by each such CSA.

- G. Click-Through Terms. For the Microsoft In-Scope Services sold and licensed to Purchasing Entities hereunder, no click-through licensing terms presented to end users or administrators, as they pertain to the delivery, operation or use of such services, shall be binding. For clarity, to the extent that certain services may present terms of use for a web portal used to administer and configure the In-Scope Services, or to download software in conjunction with the In-Scope

Services, such terms of use shall be binding, to the extent that there are no equivalent terms and conditions in the Master Agreement which pertain to the use of such web portals.

9. Definitions.

“AUP” means the section of the OST titled “Acceptable Use Policy” “Azure Consumption-Based Services” means any Microsoft Online Service made available for Purchasing Entity’s use and consumption under the Microsoft Azure Administrative Portal, following Purchasing Entity’s initial subscription order for such services, subject to consumption fees billed to Purchasing Entity (or debited against its prepaid Azure monetary commitment balance, if applicable) as described in the applicable Product Terms.

“Client” means device software, if any, that Contractor or Microsoft provides to Purchasing Entity with In-Scope Services.

“Customer Content” means the subset of Customer Data created by users, which includes the following:

- For Office 365 Services, Customer Content shall at least include Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), SharePoint Online site content and the files stored within that site, and Skype for Business Online archived conversations.
- For Microsoft Dynamics CRM Online Services, Customer Content means the entities of Customer Data managed by the Microsoft Dynamics CRM Online Services.
- For Microsoft Azure Core Services, Customer Content includes all Customer Data except as may be noted in the Microsoft Azure Trust Center (which Microsoft may update from time to time, but will not add exceptions for existing Microsoft Azure Core Services in general release).
- For Microsoft Intune Online Services, Customer Content includes all Customer Data except as may be noted in the “Data Location” section of the Microsoft Intune Trust Center.

“Customer Data” means all data, including all text, sound, or image files that are provided to Microsoft by, or on behalf of, Purchasing Entity through its use of In-Scope Services.

“DPT” means the section of the OST titled “Data Processing Terms.”

“DPT Services” means the Microsoft Online Services to which the DPT applies. As of the date this agreement was executed by the parties, DPT Services include “Microsoft Dynamics CRM Online Services,” “Office 365 Services,” “Microsoft Intune Online Services,” and “Microsoft Azure Core Services,” which consist of the following component Microsoft Online Services:

DPT Services	
Microsoft Dynamics CRM Online Services	Microsoft Dynamics CRM Online services made available through volume licensing or the Microsoft online services portal, excluding (1) Microsoft Dynamics CRM for supported devices, which includes but is not limited to Microsoft Dynamics CRM Online services for tablets and/or smartphones and (2) any separately-branded service made available with or connected to Microsoft Dynamics CRM Online, such as Microsoft Social Engagement, Parature, from Microsoft, and Microsoft Dynamics Marketing.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Exchange Online, Exchange Online Archiving, Exchange Online Protection, Advanced Threat Protection, SharePoint Online, OneDrive for Business, Project Online, Skype for Business Online, Sway, Office Online, Delve Analytics, Customer Lockbox, and Yammer Enterprise. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft’s control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded “for Office 365.”
Microsoft Azure Core Services	Cloud Services (web and worker roles), Virtual Machines (including with SQL Server), Storage (Blobs, Tables, Queues), Virtual Network, Traffic Manager, Batch, Web Sites, BizTalk Services, Media Services, Mobile Services, Service Bus, Notification Hub, Workflow Manager, Express Route, Scheduler, Multi-Factor Authentication, Active Directory, Rights Management Service, SQL Database, and HDInsight.

DPT Services	
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.

“Government Community Cloud Services” means the Microsoft Online Services identified as such (a subset of DPT Services) in the DPT and Product Terms.

“In-Scope Services” means the Microsoft Online Services for which subscription licenses are sold to Purchasing Entity by Contractor. In-Scope Services include, but are not limited to DPT Services. Except for Azure Consumption-Based Services (which are billed based upon the quantities of such services consumed by Purchasing Entity), Purchasing Entity will order individual licenses from Contractor for all In-Scope Services Licenses.

“Master Agreement” means the agreement (described therein as “NASPO ValuePoint Master Agreement for Cloud Services”) between Contractor and the Lead State, subject to the terms and conditions of the Participating Addendum between Contractor and Purchasing Entity’s State (if different from Utah), and which resulted from award of contract under Utah Solicitation Number CH16012.

“Microsoft” means Microsoft Corporation, which is subcontractor to Contractor and delivers the In-Scope Services.

“Online Services” means the Microsoft-hosted services for which Purchasing Entity acquires Licenses from Contractor hereunder.

“OST” means the Microsoft “Online Services Terms,” which are additional terms that apply to Purchasing Entity’s use of Online Services published on the Volume Licensing Site and updated from time to time, and is subject to terms and conditions in the OST which govern which version of OST is applicable to a particular subscription order.

“Portal” means the Online Services Portal for each In-Scope Service.

“Product Terms” means the document that provides information about Microsoft Products and Professional Services available through volume licensing. The Product Terms document is available on the Volume Licensing Site and is updated from time to time.

“Security Incident” means any unlawful access, use, theft or destruction to any Customer Data stored on Microsoft’s equipment or in Microsoft’s facilities, or unauthorized access to such equipment or facilities resulting in use, theft, loss, disclosure, alteration or destruction of Customer Data. All references to “Data Breach” in the Master Agreement shall be deemed to mean Security Incident.

“Service Level Agreement” (“SLA”) means the document which specifies the standards to which Microsoft agrees to adhere and by which it measures the level of service for an In-Scope Service. Microsoft’s current and archived prior version SLAs are available at the Volume Licensing Site. With respect to any In-Scope Service ordered under this Agreement, the most current SLA available at the onset of a subscription License term shall apply to that In-Scope Service for the duration of that subscription License Term, after which (for any subsequent renewal subscription License term) it will be superseded by the version current at the time of renewal.

“Subscription” means an order for a quantity of an In-Scope Service, including but not limited to (a) orders for User Subscription Licenses for one or more In-Scope Services; and (b) an order for the purpose of establishing a subscription for Azure Consumption-Based Services.

“Volume Licensing Site” means <http://www.microsoft.com/licensing/contracts> or a successor site.