Dated: 05/19/2022

ATTACHMENT A
Performance Work Statement

TABLE OF CONTENTS

1. Background

Government agencies face a highly complex and evolving marketplace when it comes to acquiring cloud products and services. Navigating security, data ownership, terms & conditions, and operational practices for acquiring and administering these solutions is a difficult and time consuming effort. GSA found through market research that common cloud requirements exist across government agencies. As a result, we are seeking to simplify and standardize cloud acquisitions through our latest effort, the Ascend Blanket Purchase Agreement (BPA).

The Ascend BPA is part of the General Services Administration's (GSA's) Cloud Marketplace vision of empowering agencies to develop and implement enterprise-level cloud acquisition strategies through a modernized and simplified approach to meet their IT and cybersecurity requirements.

The BPA will emphasize Cloud Smart / Security Smart objectives, and establish minimum baseline requirements for the acquisition, business, operations, reporting, and technology capabilities provided by commercial Cloud Service Providers (CSPs) and cloud-focused labor service providers that are not currently accessible under other GSA Multiple Award Schedule (MAS) or Governmentwide Acquisition Contracts (GWACs). The Ascend BPA will focus on enabling support for both vertical (e.g., IaaS, PaaS, SaaS) and horizontal capabilities across the ecosystem and will provide more effective system integration and managed support services for the delivery of flexible, diverse, and secure cloud solutions.

The BPA will also emphasize cybersecurity supply chain risk management (C-SCRM) and resiliency by establishing minimum cybersecurity baselines for customers to ensure their cloud solutions are compliant with applicable cybersecurity legislation, regulations, policies (e.g., Cyber Executive Order 14028), and National Institute of Standards and Technology (NIST) best practices. Integration of these requirements, along with Zero Trust Architecture (ZTA) principles will reduce the risk of evolving threats, mitigate impacts of negative cybersecurity incidents, and ensure the Confidentiality, Integrity, and Availability (CIA) for customers cloud solutions.

2. Objectives

The objective of this BPA is to provide a streamlined method for government agencies to acquire and implement secure, integrated commercial cloud service solutions, including cloud-focused labor services through the award of a BPA in accordance with FAR 8.4. These services will be epitomized by driving towards the delivery of quality services within rapid time frames, utilization of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Anything as a Services (XaaS) and related cloud Information Technology (IT) professional services to create an “open-source”-like experience. This will enable full data accessibility, ownership, and portability for the government and facilitates a government model for the reuse of common applications that would function across multiple agencies.

To achieve this goal, industry partners must be able to implement secure cloud service solutions utilizing zero trust architecture cybersecurity baselines that leverage Development, Security, and Operations (DevSecOps) and Continuous Integration/Continuous Deployment (CI/CD) agile processes that achieve results through continuous capability enhancements, minimal downtime, prompt response to emerging needs, demonstrated reliability and availability, and optimized performance with minimized resource utilization.

3. Scope

The scope of the BPA is further broken down into the following independent primary pools with respective independent sub-pools as identified by the Government. Future capability offerings and/or emerging technologies within the defined scope of the overall Pool structure requirements will be assessed for on-ramping under new sub-pool(s). **BPA Task Orders (TOs) can be placed under one or all pools as necessary for the services required.**

Pool 1: IaaS and PaaS

Consists of awardees that provide commercial cloud computing Infrastructure as a Service (IaaS) and Platform as a Service (IaaS, PaaS) solutions.

- **Sub-Pool 1-1: Unclassified Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) Cloud Service Offerings (CSOs)**
- **Sub-Pool 1-2: Classified Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) Cloud Service Offerings (CSOs)**
- **Sub-Pool 1-X: Additional sub-pools will be defined based upon government requirements.**

Pool 2: SaaS (TBD, will be added at a later date and time via the onboarding process)

Will consist of awardees that provide Government identified Software as a Service (SaaS) solutions.

- **Sub-Pool 2-X: Additional sub-pools will be defined based upon government requirements.**

Pool 3: Cloud IT Professional Services - (TBD, will be added at a later date and time via the onboarding process)

Will consist of awardees that provide cloud professional services that support the adoption of migration to, governance of, or management of commercial cloud computing solutions.

- **Sub-Pool 3-X: Additional sub-pools will be defined based upon government requirements.**

Pools / GSA Multiple Award Schedule (MAS) Special Item Number (SIN) Breakdown

Pool 1 **IaaS / PaaS**		**Pool 2** **SaaS**		**Pool 3** **Cloud Professional Services**	
Special Line Items (SINs)		Special Line Items (SINs)		Special Line Items (SINs)	
Primary	Secondary	Primary	Secondary	Primary	Secondary
518210C	Any additional awarded MAS Contract SIN determined to be necessary	518210C	Any additional awarded MAS Contract SIN determined to be necessary	518210C	54151S, along with any other additional awarded MAS Contract SIN determined to be necessary

Note: The use of any additional awarded MAS SINs is proposed to address complex or unique customer requirements associated with hybrid cloud solutions or 'on-premises' requirements that are not supported under SIN 518210C or SIN 54151S. They should not represent a significant level of effort or commodity procurement cost relative to the overall solution cost estimate.

4. References, Blanket Purchase Agreement

Authorized ordering entities and authorized vendors shall adhere to the current revisions or updates of the referenced laws, regulations, policies, specifications and standards, and related information and tools identified in Appendix I. If a future revision or update to a reference is perceived to create change(s) to the BPA, the authorized ordering entities or authorized vendors shall notify the administrative agency.

5. Identities

5.1. Administrative Agency

The administrative agency is responsible for the administration of this BPA is the General GSA, ITC.

5.1.1. Administrative Agency Responsibilities

5.1.1.1. Best In Class

Administrative agency is responsible for requesting the BIC designation from OMB for the BPA, and on designation, will manage all requirements associated with maintaining the BIC designation.[1, 2, 3]

5.1.1.2. Blanket Purchase Agreement Administration

Administrative agency is responsible for ensuring the BPA is administered in accordance with all applicable laws, regulations, policies, and T&C of the US, GSA, GSA MAS, and BPA.

5.1.1.3. Blanket Purchase Agreement Solicitations, Awards, Modifications

Administrative agency is solely responsible for the issuance of BPA solicitation(s) (i.e., sub-pools), award(s), and modification(s).

5.1.1.4. Cybersecurity Assessments and Evaluations

5.1.1.4.1. Findings and Recommendations

Administrative agency is responsible for receiving and reviewing authorized assessment and evaluation entities' independent assessment and evaluation findings and recommendations (e.g., reports).

5.1.1.4.1.1. Communications and Distribution

Administrative Agency is responsible for communicating and distributing the assessment and evaluation findings and recommendations to the following:

- DCAS
- FedRAMP

[1] M-19-13: Category Management: Making Smarter Use of Common Contract Solutions and Practices
[2] M-22-03: Advancing Equity in Federal Procurement
[3] Acquisition Gateway: Best In Class

- Impacted authorized ordering entity(ies)

5.1.1.4.1.2. Suspension and Termination of Blanket Purchase Agreement

Administrative agency is responsible for evaluating and determining if the findings and recommendations of an independent assessment and evaluation or other off-boarding events warrants the suspension or termination (i.e., termination for cause, termination for convenience) of a BPA award(s) to an authorized vendor under this BPA.

5.1.1.5. Performance Conflict Resolution

Administrative agency is responsible for arbitrating and resolving performance conflicts that are unresolvable between authorized ordering entities and authorized vendors.

5.1.1.6. Relief of Blanket Purchase Agreement Requirements

Administrative agency is solely responsible for the adjudication (e.g., approval, denial) of all requests for relief of BPA requirements from authorized ordering entities or authorized vendors.

5.2. Authorized Assessment and Evaluation Entity

An authorized assessment and evaluation entity is an explicitly identified government entity under this BPA, that is authorized to conduct and perform independent assessments and evaluations leveraging best practices and guidelines established by NIST and commercial standards.

5.2.1. United States Federal Government

The following US Federal Government agencies or subordinate agencies, components, and offices are authorized assessment and evaluation entities:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Government Accounting Office (GAO)
- National Security Administration (NSA) / Central Security Service (CSS)
- Office of the Director of National Intelligence (ODNI)

5.2.2. United States Department of Defense

The following DoD agencies or subordinate agencies, components, and offices are authorized assessment and evaluation entities:

- Director Operational Test & Evaluation (DOT&E)
- Marine Corps Forces Cyberspace Command
- Sixteenth Air Force (AFCYBER)
- US Army Cyber Command (ARCYBER)

- US Cyber Command (USCC)
- US Fleet Cyber Command

5.2.3. Authorized Assessment and Evaluation Entity Responsibilities

5.2.3.1. Cybersecurity Assessments and Evaluations

Authorized assessment and evaluation entities are responsible for conducting and performing announced and unannounced independent cybersecurity (e.g., Central Intelligence Agency (CIA) triad) and operational (e.g., performance, SLAs) assessments and evaluations (e.g., OT&E) of the cloud services (i.e., IaaS, PaaS, SaaS) architectures (e.g., compute, networking, storage) and security domains involved in the processing, transporting, and / or storing authorized ordering entities data.

5.2.3.1.1. Coordination

Authorized assessment and evaluation entities are responsible for coordinating assessment and evaluation activities with the authorized vendors. Coordination responsibilities shall include planning, execution, and post assessment and evaluation activities (e.g., remediations, Plan of Actions and Milestones (POA&Ms).

5.2.3.1.2. Costs

Authorized assessment and evaluation entities are responsible for their assessment and evaluation costs.

5.2.3.1.3. Findings and Recommendations

Authorized assessment and evaluation entities are responsible for documenting the assessment and evaluation findings and recommendations (e.g., reports).

5.2.3.1.3.1. Communications and Distribution

Authorized assessment and evaluation entities are responsible for communicating and distributing the assessment and evaluation findings and recommendations to the following:

- BPA Contracting Officer
- Authorized assessment and evaluation entities
- Assessed and evaluated authorized vendor(s)

5.2.3.1.3.2. Information Classification Levels

Authorized assessment and evaluation entities are responsible for establishing the information classification level (i.e., Controlled Unclassified Information (CUI), Confidential, Secret, Top Secret) of the assessment and evaluation findings and recommendations.

Table 1: Minimum Information Classification Levels	
Authorization Level	**Minimum Information Classification Level**
DCAS Authorization IL 2	CUI
DCAS Authorization IL 4	CUI
DCAS Authorization IL 5	Confidential
DCAS Authorization IL 6	Secret
FedRAMP Moderate	CUI
FedRAMP High	CUI

5.2.3.1.3.3. Information Classification Markings

Authorized assessment and evaluation entities are responsible for identifying and applying the correct information classification markings[4] to the assessment and evaluation findings and recommendations.

5.2.3.1.3.4. Public Disclosure and Release

Authorized assessment and evaluation entities are responsible for developing an unclassified version (i.e., sensitive information redacted) of the assessment and evaluation findings (e.g., reports) and recommendations suitable for public disclosure and release.

Authorized assessment and evaluation entities are responsible for the public disclosure and release of the unclassified versions of the assessment and evaluation findings and recommendations in accordance with applicable laws,[5] regulations, and policies.

Authorized assessment and evaluation entities are responsible for issuing written notifications to the assessed and evaluated authorized vendor(s) a minimum of 30 calendar days prior to the date of public disclosure or release of the unclassified version of the assessment and evaluation findings and recommendations.

Authorized assessment and evaluation entities are responsible for including a copy of the unclassified version of the assessment and evaluation findings and recommendations with the notifications.

[4] Controlled Unclassified Information (CUI) Markings List

[5] 5 U.S.C. 552 GOVERNMENT ORGANIZATION AND EMPLOYEES, Public information; agency rules, opinions, orders, records, and proceedings

5.2.3.1.4. Techniques

Authorized assessment and evaluation entities are responsible for determining the appropriate active (e.g., ethical hacker, red team, penetration testing) and passive (e.g., emulation, simulation) assessment and evaluation techniques.

5.3. Authorized Ordering Entity

An authorized ordering entity is a federal, state, or local government agency or other eligible entity that is authorized to use the GSA MAS Federal Supply Schedule (FSS).

Authorization to use the GSA MAS FSS are per the following laws, regulations, and policies:

Table 2: GSA MAS FSS Authorized Ordering Entities	
A	40 U.S.C. 502 PUBLIC BUILDINGS, PROPERTY, AND WORKS, Services for other entities[6, 7, 8, 9, 10]
B	GSA Order 4800.2I "Eligibility to Use GSA Sources of Supply and Services"
	— Appendix A: Executive Agencies
	— Appendix B: Other Eligible Users
	— Appendix C: International Organizations and Others Determined Eligible under Section 607 of the Foreign Assistance Act

5.3.1. Cooperative Purchasing Program

Authorized ordering entities, per 40 U.S.C. 502(c), may leverage this BPA under the GSA Cooperative Purchasing Program.

5.3.2. Disaster Purchasing Program

Authorized ordering entities, per 40 U.S.C. 502(c), may leverage this BPA under the GSA Disaster Purchasing Program to facilitate disaster preparation, response, or major disaster recovery.[11]

[6] Codified: E-Government Act of 2002
[7] Codified: Federal Supply Schedules Usage Act of 2010
[8] Codified: John Warner National Defense Authorization Act for Fiscal Year 2007
[9] Codified: Local Preparedness Acquisition Act
[10] Codified: Robert T. Stafford Disaster Relief and Emergency Assistance Act
[11] Emergency Acquisitions Guide

A disaster may be natural or man-made, including acts of terrorism (e.g., biological, chemical, nuclear, radiological).

TO award(s) in support of major disaster recovery shall be in direct response to a Robert T. Stafford Disaster Relief and Emergency Assistance Act (i.e., Stafford Act) Presidential declaration.

Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) maintains and manages the list of Stafford Act declared disasters.[12]

5.3.3. Authorized Ordering Entity Responsibilities

5.3.3.1. Cybersecurity Assessments and Evaluations

5.3.3.1.1. Coordination

Authorized ordering entities are responsible for coordinating (e.g., requesting) assessment and evaluation activities with their respective authorized assessment and evaluation entity(ies).

5.3.3.1.2. Findings and Recommendations

Authorized ordering entities are responsible for receiving and reviewing authorized assessment and evaluation entities' assessment and evaluation findings and recommendations (e.g., reports).

5.3.3.1.2.1. Suspension and Termination of Task Order(s)

Authorized ordering entities are responsible for evaluating and determining if the findings and recommendations of an assessment and evaluation warrants the suspension or termination (i.e., termination for cause, termination for convenience) of a TO(s) awarded under this BPA.

5.3.3.2. Cybersecurity Authorization To Operate (ATO)

Authorized ordering entities are responsible for the issuance of ATO(s) for the authorized ordering entity's leveraged cloud services (i.e., IaaS, PaaS, SaaS) in accordance with applicable laws, regulations, and policies.

[12] Declared Disasters: https://www.fema.gov/disaster/declarations

5.3.3.2.1. Department of Defense Cloud Authorization Services (DCAS) and Federal Risk and Authorization Management Program Reporting

Authorized ordering entities are responsible for reporting and submitting issued ATO(s) to DCAS and FedRAMP.

Authorized ordering entities are responsible for reporting and submitting any ATO Assessment & Authorization (A&A) identified inconsistencies (i.e., with FedRAMP authorization, with DCAS authorization), concerns, or issues to DCAS and FedRAMP.

5.3.3.2.2. Suspension and Termination of Task Order(s)

Authorized ordering entities are responsible for evaluating and determining if the findings and recommendations of an ATO A&A warrants the suspension or termination (i.e., termination for cause, termination for convenience) of a TO(s) awarded under this BPA.

5.3.3.3. Cybersecurity Incident Reporting

Authorized ordering entities are responsible for timely reporting cybersecurity incidents to the BPA Contracting Officer and to their TO(s) authorized vendors to ensure the authorized vendor can take appropriate mitigating actions.

5.3.3.4. Cybersecurity Testing

Authorized ordering entities are responsible for conducting and performing cybersecurity (e.g., CIA triad) and operational (e.g., performance, SLAs) testing of the authorized ordering entities' solutions (e.g., applications, configurations, databases, services, software, websites) deployed and operating within the cloud services (i.e., IaaS, PaaS, SaaS) processing, transporting, and / or storing authorized ordering entities data.

5.3.3.4.1. Testing Impacts

Authorized ordering entities are responsible for ensuring that authorized ordering entities cybersecurity testing activities do not negatively impact the authorized vendors cloud services (i.e., IaaS, PaaS, SaaS) operations, performance, or security.

5.4. Authorized Reseller

An authorized reseller is an entity that has been explicitly authorized (e.g., contractual agreement) by a CSP(s) to act as an authorized agent or intermediary (e.g., cloud broker) to offer, negotiate, and sell, on the behalf of the CSP, the CSP's cloud services.

5.4.1. Authorized Reseller Responsibilities

5.4.1.1. Legal Authority(ies) Blanket Purchase Agreement

Authorized resellers shall be responsible for ensuring they have the vested authority to contractually commit the CSP(s) to the applicable laws, regulations, policies, and Terms & Conditions (T&Cs) of the US, GSA, GSA MAS, and BPA prior to submission of any proposal(s) in response to a BPA solicitation(s).

5.4.1.2. Legal Authority(ies) Task Order(s)

Authorized resellers shall be responsible for ensuring they have the vested authority to contractually commit the CSP(s) to the applicable laws, regulations, policies, and T&C of the US, GSA, GSA MAS, BPA, and TO(s) prior to submission of any proposal(s) in response to a TO solicitation(s).

5.4.1.3. Notification of Relationship Change(s)

Authorized resellers shall be responsible for immediately notifying the BPA Contracting Officer on any changes to the relationship (e.g., business, contractual) between the authorized reseller and CSP(s) (e.g., no longer an authorized reseller).

5.4.1.4. Notification of Terms and Conditions Discrepancies

Authorized resellers shall be responsible for immediately notifying the BPA Contracting Officer when a conflict, discrepancy, or issue is identified between the applicable laws, regulations, policies, and T&Cs of the US, GSA, GSA MAS, BPA, or TO(s) and the CSP(s).

5.4.1.5. Verified Product Portal (VPP)

Authorized resellers shall be responsible for ensuring they have been appropriately and correctly identified, listed, and maintained by the CSP(s) in the GSA VPP.

5.5. Authorized Vendor

An authorized vendor is an entity that has been awarded a BPA award by the BPA Administering function. An authorized vendor can be either a CSP or an authorized reseller.

5.5.1. Authorized Vendor Responsibilities

5.5.1.1. Cybersecurity Assessments and Evaluations

5.5.1.1.1. Coordination

Authorized vendors shall be responsible for coordinating assessment and evaluation activities with the authorized assessment and evaluation entities. Coordination responsibilities shall include planning, execution, and post assessment and evaluation activities (e.g., remediations, POA&Ms).

5.5.1.1.2. Costs

Authorized vendors shall be responsible for their assessment and evaluation costs.

5.5.1.1.3. Findings and Recommendations

Authorized vendors shall be responsible for receiving and reviewing authorized assessment and evaluation entities' assessment and evaluation findings and recommendations (e.g., reports).

5.5.1.1.4. Mitigation and Remediation

Authorized vendors shall be responsible for evaluating, determining, and executing the appropriate mitigation and remediation activities (e.g., fixes, patches, updates) in response to the findings and recommendations of an assessment and evaluation.

5.5.1.1.5. Public Disclosure and Release

Authorized vendors shall be responsible for reviewing the written notifications from authorized assessment and evaluation entities including the provided unclassified versions of the assessment and evaluation findings and recommendations and timely reply, within 30 calendar days, to the authorized assessment and evaluation entities of any concerns or objections to the public disclosure or release.

5.5.1.2. Cybersecurity Authorization To Operate (ATO)

5.5.1.2.1. Coordination

Authorized vendors shall be responsible for coordinating ATO A&A activities with the authorized ordering entities. Coordination responsibilities shall include planning, execution, and post assessment and evaluation activities (e.g., mitigations, remediations, POA&Ms).

5.5.1.2.2. Costs

Authorized vendors shall be responsible for their ATO A&A costs.

5.5.1.2.3. Findings and Recommendations

Authorized vendors shall be responsible for receiving and reviewing authorized ordering entities' ATO A&A findings and recommendations (e.g., reports).

5.5.1.2.4. Mitigation and Remediation

Authorized vendors shall be responsible for evaluating, determining, and executing the appropriate mitigation and remediation activities (e.g., fixes, patches, updates) in response to the findings and recommendations of an ATO A&A.

5.5.1.3. Notification of Terms and Conditions Discrepancies

Authorized vendors shall be responsible for immediately notifying the BPA Contracting Officer when a conflict, discrepancy, or issue is identified between the applicable laws, regulations, policies, and T&Cs of the US, GSA, GSA MAS, BPA, or their TO(s).

5.5.1.4. Performance Conflict Elevation

Authorized vendors shall be responsible for elevating unresolvable performance conflicts with authorized ordering entities to the BPA Contracting Officer for arbitration and resolution.

5.6. Cloud Service Provider

A CSP is an entity that directly operates and manages the cloud services (i.e., IaaS, PaaS, SaaS) technology (e.g., facility, hardware, software).

5.6.1. Cloud Service Provider Responsibilities

5.6.1.1. Cloud Services, Infrastructure as a Service

CSPs providing IaaS cloud services are generally responsible for the Operations and Maintenance (O&M) of the data center (e.g., physical security, environment monitoring), network (e.g., routing, switching), storage (e.g., archive, cache, primary, secondary), servers (e.g., CPU, RAM), and virtualization (e.g., hypervisor, virtual machines).

5.6.1.2. Cloud Services, Platform as a Service

CSPs providing PaaS cloud services are generally responsible for the O&M of the data center, network, storage, servers, virtualization, operating system, database, and security (e.g., cybersecurity, Information Assurance).

5.6.1.3. Cloud Services, Software as a Service

CSPs providing SaaS cloud services are generally responsible for the O&M of the data center, network, storage, servers, virtualization, operating system, database, security, and applications (e.g., office productivity, accounting).

5.6.1.4. Department of Defense Cloud Authorization Services Authorization(s)

CSPs shall be responsible for obtaining and maintaining DCAS authorization(s) for their CSO(s) (i.e., IaaS, PaaS, SaaS) in accordance with DCAS regulations and policies.

5.6.1.5. Federal Risk and Authorization Management Program Authorization(s)

CSPs shall be responsible for obtaining and maintaining FedRAMP authorization(s) for their CSO(s) (i.e., IaaS, PaaS, SaaS) in accordance with FedRAMP regulations and policies.

5.6.1.6. Legal Authority(ies) Blanket Purchase Agreement

CSPs shall be responsible for ensuring the authorized reseller(s) have the vested authority to contractually commit the CSP to the applicable laws, regulations, policies, and T&C of the US, GSA, GSA MAS, and BPA prior to submission of any proposal(s) in response to a BPA solicitation(s).

5.6.1.7. Legal Authority(ies) Task Order(s)

CSPs shall be responsible for ensuring the authorized reseller(s) have the vested authority to contractually commit the CSP to the applicable laws, regulations, policies, and T&C of the US, GSA, GSA MAS, BPA, and TO(s) prior to submission of any proposal(s) in response to a TO solicitation(s).

5.6.1.8. Notification of Ownership Change(s)

CSPs shall be responsible for notifying the BPA Contracting Officer at least 90 calendar days prior to any changes to their ownership structure.

Changes in ownership structure include but are not limited to:

- Sale or fraction thereof to foreign entities (e.g., business, corporation, sovereign wealth fund) or non-US citizens (i.e., foreigner).
- Merger with foreign entities (e.g., business, corporation, sovereign wealth fund) or non-US citizens (i.e., foreigner).

- Significant changes in foreign entities (e.g., business, corporation, sovereign wealth fund) or non-US citizens (i.e., foreigner) control or influence (e.g., board members, loans, partnership, stock ownership).

5.6.1.9. Notification of Relationship Change(s)

CSPs shall be responsible for immediately notifying the BPA Contracting Officer on any changes to the relationship (e.g., business, contractual) between the CSP and their authorized reseller(s) (e.g., no longer an authorized reseller).

5.6.1.10. Notification of Terms and Conditions Discrepancies

CSPs shall be responsible for immediately notifying the BPA Contracting Officer when a conflict, discrepancy, or issue is identified between the applicable laws, regulations, policies, and T&C of the US, GSA, GSA MAS, BPA, or TO(s) and the CSP.

5.6.1.11. Verified Product Portal

CSPs shall ensure they have appropriately and correctly identified, listed, and maintained their authorized reseller(s) in the GSA VPP.

5.7. Department of Defense Cloud Authorization Services

DCAS supports the DoD with a standardized approach to security assessments, authorizations, and continuous monitoring for cloud services (i.e., IaaS, PaaS, SaaS).

5.7.1. Department of Defense Cloud Authorization Services Responsibilities

5.7.1.1. Cybersecurity Assessments and Evaluations

5.7.1.1.1. Findings and Recommendations

DCAS is responsible for receiving and reviewing authorized assessment and evaluation entities' assessment and evaluation findings and recommendations (e.g., reports).

5.7.1.1.1.1. Suspension and Termination of Authorization(s)

DCAS is responsible for evaluating and determining if the findings and recommendations of an assessment and evaluation warrants the suspension or termination of a DCAS authorization(s) for a CSO(s).

5.7.1.1.1.1.1. Suspension and Termination Communications

DCAS is responsible for communicating to the BPA Contracting Officer, CSPs, and authorized ordering entities that DCAS has suspended or terminated a DCAS authorization for a CSO(s).

5.7.1.2. Cybersecurity Authorization To Operate (ATO)

5.7.1.2.1. Findings and Recommendations

DCAS is responsible for receiving and reviewing authorized ordering entities reported ATO A&A inconsistencies (i.e., with DCAS authorization), concerns, and issues.

5.7.1.2.1.1. Suspension and Termination of Authorization(s)

DCAS is responsible for evaluating and determining if the authorized ordering entities' ATO A&A inconsistencies (i.e., with DCAS authorization), concerns, or issues warrant the suspension or termination of a DCAS authorization(s) for a CSO(s).

5.7.1.2.1.2. Suspension and Termination Communications

DCAS is responsible for communicating to the BPA Contracting Officer, CSPs, and authorized ordering entities that DCAS has suspended or terminated a DCAS authorization for a CSO(s).

5.7.1.3. Department of Defense Cloud Authorization Services Authorization

DCAS is solely responsible for the issuance, monitoring, and revocation of DCAS authorizations for CSOs.

5.7.1.3.1. Department of Defense Cloud Authorization Services Impact Level

DCAS is solely responsible for the DCAS authorization Impact Level (IL) (i.e, 2, 4, 5, 6) for DCAS authorized CSOs.

5.7.1.3.2. Department of Defense Cloud Authorization Services Service Model Classification

DCAS is solely responsible for the DCAS service model classification (i.e, IaaS, PaaS, SaaS) for DCAS authorized CSOs.

5.8. Federal Risk and Authorization Management Program

FedRAMP is a US Government-wide program that provides a standardized approach to security assessments, authorizations, and continuous monitoring for cloud services (i.e., IaaS, PaaS, SaaS).

5.8.1. Federal Risk and Authorization Management Program Responsibilities

5.8.1.1. Cybersecurity Assessments and Evaluations

5.8.1.1.1. Findings and Recommendations

FedRAMP is responsible for receiving and reviewing authorized assessment and evaluation entities' assessment and evaluation findings and recommendations (e.g., reports).

5.8.1.1.1.1. Suspension and Termination of Authorizations

FedRAMP is responsible for evaluating and determining if the findings and recommendations of an assessment and evaluation warrants the suspension or termination of a FedRAMP authorization(s) for a CSO(s).

5.8.1.1.1.1.1. Suspension and Termination Communications

FedRAMP is responsible for communicating to the BPA Contracting Officer, CSPs, and authorized ordering entities that FedRAMP has suspended or terminated a FedRAMP authorization for a CSO(s).

5.8.1.2. Cybersecurity Authorization To Operate

5.8.1.2.1. Findings and Recommendations

FedRAMP is responsible for receiving and reviewing authorized ordering entities reported ATO A&A inconsistencies (i.e., with FedRAMP authorization), concerns, and issues.

5.8.1.2.1.1. Suspension and Termination of Authorization(s)

FedRAMP is responsible for evaluating and determining if the authorized ordering entities' ATO A&A inconsistencies (i.e., with FedRAMP authorization), concerns, or issues warrant the suspension or termination of a FedRAMP authorization(s) for a CSO(s).

5.8.1.2.1.1.1. Suspension and Termination Communications

FedRAMP is responsible for communicating to the BPA Contracting Officer, CSPs, and authorized ordering entities that FedRAMP has suspended or terminated a FedRAMP authorization for a CSO(s).

5.8.1.3. Federal Risk and Authorization Management Program Authorization

FedRAMP is solely responsible for the issuance, monitoring, and revocation of FedRAMP authorizations for CSOs.

5.8.1.3.1. Federal Risk and Authorization Management Program Impact Level

FedRAMP is solely responsible for the FedRAMP authorization IL (i.e, Light ImpactI-SaaS, Low, Moderate, High) for FedRAMP authorized CSOs.

5.8.1.3.2. Federal Risk and Authorization Management Program Service Model Classification

FedRAMP is solely responsible for the FedRAMP service model classification (i.e, IaaS, PaaS, SaaS) for FedRAMP authorized CSOs.

6. Blanket Purchase Agreement Parameters

6.1. Associate Contractor Agreement (ACA)

Authorized vendors may be required to enter into ACA for TO(s) awarded under this BPA requiring joint participation in the accomplishment of the authorized ordering entities' requirement.

The agreements shall include the basis for sharing information, data, technical knowledge, expertise, or resources.

ACA shall include the following minimum information:

- Identify the associate contractors (e.g., authorized vendors) and their relationships.
- Identify the cloud services (i.e., IaaS, PaaS, SaaS) involved and the relevant contracts (e.g., TOs) of the associate contractors.
- Describe the associate contractor’s interfaces by general subject matter.
- Identify for information to be accessed, exchanged, and / or supported:
    - Categories of information (e.g., business, financial, operational, PII, proprietary, security, technical).
    - Classification of information (i.e., Unclassified, CUI, Confidential, Secret, Top Secret).

- Ownership of information (e.g., associate contractor, government agency).
- Access means and mechanisms for information (e.g., APIs, Electronic DIs).
- Access controls means and mechanisms for the information.
- Retention and destruction policies for the information.

- Include the expiration date (or event) of the ACA.
- Identify potential conflicts between relevant contracts (e.g., TOs) and the ACA.
- Include agreements on protection of proprietary data and restrictions on employees.

Authorized vendors shall provide copies of ACA to:

- TO(s) ACO(s);
- TO(s) ISR(s);[13]
- Authorized Ordering Entities' CDO(s);
- Authorized Ordering Entities' CIO(s); and
- Authorized Ordering Entities' CISO(s)

for review and approval prior to execution of the ACA by associate contractors.

Authorized vendors shall ensure all data and information sharing is in accordance with BPA and TO(s) data and cybersecurity requirements.

Authorized vendors are not relieved of any BPA or TO(s) requirements or entitled to any adjustments to the BPA or TO(s) because of a failure to resolve a disagreement with an associate contractor.

Liability for the improper disclosure of any proprietary data contained in or referenced by any ACA shall rest with the parties to the ACA, and not the authorized ordering entities.

6.1.1. Task Order(s), Associate Contractor Agreements

All costs associated with the ACA are to be included in authorized vendors' proposals and / or negotiated costs at the TO level.

Authorized ordering entities are responsible for identifying their ACA requirements (e.g., contractors) at the TO level.

6.2. Clearance Levels - Facility

Facility Clearance Levels (FCLs) for the BPA are defined as follows:

6.2.1. United States Federal Government

Table 3: US Federal Government Facility Clearance Levels

[13] Facility Clearance

Facility Clearance Level	Definition
None	Authorized vendor has been awarded a TO requiring no access to Confidential, Secret, or Top Secret information.
Confidential	Authorized vendor has been awarded a Confidential TO requiring access to Confidential information.
Secret	Authorized vendor has been awarded a Secret TO requiring access to Secret information.
Top Secret	Authorized vendor has been awarded a Top Secret TO requiring access to Top Secret information.

6.2.2. Task Order(s), Clearance Levels - Facility

Authorized ordering entities are responsible for identifying their facility clearance requirements at the TO level.

6.3. Clearance Levels - Personnel

Authorized vendors' persons (e.g., employees, representatives, sub-contractors) may be required to successfully complete an investigation and obtain the issuance of a clearance level (e.g., security clearance) based on the authorized vendors' persons' (e.g., employees, representatives, sub-contractors) access or permissions to sensitive information or information Systems (IS).

Personnel clearance levels for the BPA are defined as follows:

6.3.1. United States Federal Government

Table 4 US Federal Government Personnel Clearance Levels

Clearance Level	Investigations
Tier 1 (T1) Non-Sensitive Positions - Low Risk	National Agency Check and Inquiries (NACI)
Tier 2 (T2) Non-Sensitive Public Trust Positions - Moderate Risk	Moderate Risk Background Investigation (MBI)
Tier 4 (T4) Non-Sensitive Public Trust Positions - High Risk	Background Investigation (BI)

Tier 3 (T3) National Security Positions - Secret / Confidential Clearance	National Agency Check with Law and Credit (NACLC)
Tier 5 (T5) National Security Positions - Top Secret Clearance	Single Scope Background Investigation (SSBI)

6.3.1.1. Security Clearance Reciprocity

United States Federal Government authorized ordering entities shall accept via reciprocity security clearances adjudicated and issued by authorized investigative services (e.g., DCSA) in accordance with *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Public Law 108-458, Sec. 3001 Security clearances*.

6.3.2. Task Order(s), Clearance Levels - Personnel

Authorized ordering entities are authorized to identify additional personnel clearance level requirements at the TO level.

6.4. Commercial Products

The procurement of "commercial products",[14] inclusive of active and passive hardware appliances and devices, are not authorized to be procured under this BPA.

6.5. Commercial Services

All cloud services (i.e., IaaS, PaaS, SaaS) and cloud related IT professional services offered under this BPA by authorized vendors and procured under awarded TO(s) by authorized ordering entities shall be categorized and classified as "commercial services" as defined by 41 U.S.C. 103a [15] and *FAR 2.101* [16] and shall adhere to all applicable federal acquisitions

[14] FAR 2.101 Definitions, Commercial product
[15] 41 U.S.C. 103a PUBLIC CONTRACTS, Commercial Service
[16] FAR 2.101 Definitions, Commercial service

laws,[17, 18, 19, 20, 21, 22, 23, 24] regulations,[25, 26] and policies pertaining to the acquisition of "commercial services."

Cloud services and cloud related IT professional services shall be:

- Funded at time of services execution (e.g., service delivery).
- Furnished (e.g., service delivery) only within executed PoPs (i.e., PoP start date - PoP end date).
- Paid for in arrears.[27]

6.6. Contractor Team Arrangements (CTAs)

The allowance or non-allowance of CTAs at the BPA award level will be per the following table:

Table 5: BPA Contractor Team Arrangements

Allowed / Not Allowed	Pool	Title
Not Allowed	1	Infrastructure as a Service, Platform as a Service
Not Allowed	1-1	Unclassified Infrastructure as a Service, Platform as a Service
Not Allowed	1-2	Classified Infrastructure as a Service, Platform as a Service
Not Allowed	2	Software as a Service
Allowed	3	Cloud Related IT Professional Services

[17] 10 U.S.C. 2306c ARMED FORCES, Multiyear contracts: acquisition of services
[18] 10 U.S.C. 2410a ARMED FORCES, Contracts for periods crossing fiscal years: severable service contracts; leases of real or personal property
[19] 31 U.S.C. 3324 MONEY AND FINANCE, Advances
[20] 41 U.S.C. 3902 PUBLIC CONTRACTS, Severable services contracts for periods crossing fiscal years
[21] 41 U.S.C. 3903 PUBLIC CONTRACTS, Multiyear contracts
[22] Principles of Federal Appropriations Law
[23] Principles of Federal Appropriations Law, Volume I, Chapter 5 Availability of Appropriations: Time, B. The Bona Fide Needs Rule
[24] Principles of Federal Appropriations Law, Volume II, Chapter 6 Availability of Appropriations: Amount, C. The Antideficiency Act
[25] FAR 2.101 Definitions
[26] 13 CFR 121.1203(d)(3) When will a waiver of the Nonmanufacturer Rule be granted for an individual contract?
[27] 31 U.S.C. 3324 MONEY AND FINANCE, Advances

Note: This BPA restricts more than one authorized vendor to deliver a single CSP's CSOs (i.e., cloud service catalog). Therefore, CTAs within Pool 1 and Pool 2 for a single CSP are not allowed. If a multiple CSP solution (e.g., multi-cloud solution) is required by an authorized ordering agency, then a CTA between different ASCEND BPA authorized vendors would be allowed at the TO level to meet the authorized ordering entities requirements.

6.6.1. Task Order(s), Contractor Teaming Arrangements

The allowance or non-allowance of CTAs at the TO level will be per the following table:

Table 6: TO Contractor Team Arrangements

Allowed / Not Allowed	Pool	Title
Allowed (Hybrid / Multi-Cloud)	1	Infrastructure as a Service, Platform as a Service
Allowed (Hybrid / Multi-Cloud)	1-1	Unclassified Infrastructure as a Service, Platform as a Service
Allowed (Hybrid / Multi-Cloud)	1-2	Classified Infrastructure as a Service, Platform as a Service
Allowed (Multiple Applications)	2	Software as a Service
Allowed	3	Cloud Related IT Professional Services

Note: This BPA restricts more than one authorized vendor to deliver a single CSP's CSOs (i.e., cloud service catalog). Therefore, CTAs within Pool 1 and Pool 2 for a single CSP are not allowed. If a multiple CSP solution (e.g., multi-cloud solution) is required by an authorized ordering agency, then a CTA between different ASCEND BPA authorized vendors would be allowed at the TO level to meet the authorized ordering entities requirements.

6.7. Cooperative Purchasing Program

Authorized vendors may be authorized and participate in the Cooperative Purchase Program under *MAS SIN 518210C Cloud Computing and Cloud Related IT Professional Services*.

6.8. Disaster Purchasing Program

Authorized vendors may be authorized and participate in the Disaster Purchase Program under *MAS SIN 518210C Cloud Computing and Cloud Related IT Professional Services*.

6.8.1. Task Order(s), Disaster Purchasing Program

TO award(s) under the Disaster Purchasing Program shall include the following language:

This order is placed under GSA Federal Supply Schedule number <Insert Number Here> under the authority of the GSA Disaster Purchasing program. The products and services purchased will be used in preparation or response to disasters or recovery from major disaster declared by the President, or recovery from terrorism or nuclear, biological, chemical, or radiological attack.

6.9. Utilization Based Discounts

Authorized vendors may offer and propose utilization-based discounts, at the BPA TO award level, that allows authorized ordering entities to earn utilization-based discounts in one PoP and apply those discounts to the next PoP (e.g., option period) for cloud services (i.e., IaaS, PaaS, SaaS).[28, 29]

Utilization based discounts shall comply with the following conditions:

- Earning utilization-based discounts cannot be contingent or otherwise dependent on an authorized ordering entity executing the next PoP.
    - The utilization-based discounts are null and void and have no monetary value if an authorized ordering entity decides not to execute a future PoP.
- Authorized ordering entities shall retain the independent right to determine if it is advantageous (i.e., in the best interest) for the authorized ordering entity to execute a PoP.[30]
    - Authorized ordering entities are allowed to consider the earned utilization-based discounts as part of the authorized ordering entities' advantageous evaluations.
- Earning utilization-based discounts must be based on the direct utilization of cloud services by authorized ordering entities.
    - Utilization-based discounts can be based on authorized ordering entities reaching usage thresholds or tiers for cloud services.
    - Utilization-based discounts can be based on the difference between TO awarded price and actual cost differences (e.g., cost avoidance, cost savings, price reductions) for cloud services.
    - Utilization-based discounts can be based on temporary generally available promotions (e.g., sales).
    - Utilization-based discounts cannot be based on unexpensed obligations.
- Earned utilization-based discounts do not modify or otherwise change the TO awarded prices for cloud services.
    - Authorized vendors shall invoice authorized ordering entities for cloud services based on TO awarded prices.
    - Authorized ordering entities shall pay invoices based on TO awarded prices.

[28] Principles of Federal Appropriations Law, Volume I, Chapter 5 Availability of Appropriations: Time, B. The Bona Fide Needs Rule, 8. Multiyear Contracts, c. Fiscal Year Appropriations
[29] B-164908(2), JANUARY 31, 1969, 48 COMP. GEN. 497
[30] FAR 17.207 Exercise of Options

- Utilization-based discounts are compatible and combinable with Requirements Contracts[31]
- Earned utilization-based discounts are at the CLIN level.
  - Earned utilization-based discounts must be applied to similarly scoped CLINs (e.g., Compute CLIN to Compute CLIN) in the next PoP.
  - Earned-utilization based discounts applied to the next PoP are applied first to costs incurred.
  - Earned-utilization based discounts have no monetary value and are null and void at the end of TO performance period.
  - Earned-utilization based discounts are not federal appropriations (e.g., 1 year, No Year appropriations).

6.10. Government-Furnished Information (GFI)

The provisions affecting GFI under this BPA shall be in accordance with *FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems*.

Authorized vendors may be issued or granted access to GFI.

Authorized vendors shall be responsible and accountable for all GFI and shall take all reasonable precautions and such other actions as may be directed by the authorized ordering entities, or in the absence of such direction, in accordance with sound business practice to secure, safeguard, and protect GFI in the authorized vendors possession or custody.

Authorized vendors shall not use GFI for any other purposes than those described in their awarded TO(s).

Authorized vendors shall not mark or affix any decals, emblems, or watermarks portraying the authorized vendor's name or logo to GFI except as directed by the authorized ordering entities.

Authorized vendors shall not remove any markings or affixed decals, emblems, or watermarks (e.g., classification markings) from the GFI except as directed by the authorized ordering entities.

Authorized vendors shall not remove GFI from authorized ordering entities IS, facilities, or other supported areas without the review and written approval of the authorized ordering entities.

Authorized vendors shall not distribute, publish, or otherwise share or grant access to GFI with third parties or unauthorized parties without the review and written approval of the authorized ordering entities

[31] FAR 16.503 Requirements contracts

6.10.1. Controlled Unclassified Information

Authorized vendors may be issued or granted access to CUI.

Authorized vendors shall be responsible and accountable for all CUI and shall ensure CUI is secure, safeguarded, and protected in accordance with *NIST, SP 800-171 Rev.2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,*[32] *NIST, SP 800-172: Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171* and *DoDI 8582.01: Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information.*[33]

6.10.2. Task Order(s), Government-Furnished Information

Authorized ordering entities are authorized to identify additional GFI requirements at the TO level. [34, 35]

6.11. Government-Furnished Property (GFP)

The provisions affecting GFP under this BPA shall be in accordance with *FAR 52.245-1 Government Property*.

Authorized vendors may be issued GFP that includes both real (e.g., laptops, mobile devices) and digital property (e.g., accounts, certificates, security tokens) and GFI.

Authorized vendors shall be responsible and accountable for all GFP and shall take all reasonable precautions and such other actions as may be directed by the authorized ordering entities, or in the absence of such direction, in accordance with sound business practice to secure, safeguard, and protect GFP in the authorized vendors possession or custody.

Authorized vendors shall not use GFP for any other purposes than those described in their awarded TO(s).

Authorized vendors shall not mark or affix any decals, emblems, or signs portraying the authorized vendor's name or logo to GFP except as directed by the authorized ordering entities.

Authorized vendors shall not remove any markings or affixed decals, emblems, or signs (e.g., classification markings) from the GFP except as directed by the authorized ordering entities.

[32] NIST, SP 800-171A: Assessing Security Requirements for Controlled Unclassified Information
[33] DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
[34] DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
[35] DFARS 252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends

Authorized vendors shall not remove GFP from authorized ordering entities facilities or other supported areas without the review and written approval of the authorized ordering entities.

Authorized vendors shall not provide or otherwise share or grant access to GFP with third parties or unauthorized parties without the review and written approval of the authorized ordering entities.

6.11.1. Task Order(s), Government-Furnished Property

Authorized ordering entities are authorized to identify additional GFP requirements at the TO level

6.12. Geographic Locations

Geographic locations for the BPA are defined as follows:

Table 7: Geographic Locations

Geographic Location	Definition
CONUS	Contiguous 48 states and the DC
GSA Region 1 New England	Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont
GSA Region 2 Northeast and Caribbean	New Jersey, New York, Puerto Rico, Virgin Islands
Region 3 Mid-Atlantic	Delaware, Maryland, Pennsylvania, Virginia, West Virginia
GSA Region 4 Southeast Sunbelt	Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee
GSA Region 5 Great Lakes	Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin
GSA Region 6 The Heartland	Iowa, Kansas, Missouri, Nebraska
GSA Region 7 Greater Southwest	Arkansas, Louisiana, New Mexico, Oklahoma, Texas
GSA Region 8 Rocky Mountain	Colorado, Montana, North Dakota, South Dakota, Utah, Wyoming
GSA Region 9 Pacific Rim	American Samoa, Arizona, California, Guam, Hawaii, Nevada

GSA Region 10 Northeast Arctic	Alaska, Idaho, Oregon, Washington
GSA Region 11 National Capital	Washington, District of Columbia (DC), Metropolitan Area
OCONUS	Africa, Alaska, Antarctica, Asia, Australia, Canada, Caribbean, Central America, Europe, Greenland, Hawaii, Middle East, Mexico, Oceania, South America

6.12.1. Task Order(s), Geographic Locations Requirements

Authorized ordering entities should identify their geographic locations or subset thereof (e.g., state, metropolitan area) requirements at the TO level.

6.13. Information Classification Levels

Information classification levels for the BPA are defined as follows:

6.13.1. United States Federal Government

Table 8: US Federal Government Information Classification Levels

Information Classification Level	Definition
Unclassified	Information that is authorized for public disclosure.
Controlled Unclassified Information	Information that requires by a law, regulation, or Government-wide policy safeguarding or dissemination controls.
Confidential	Information that the unauthorized disclosure of which reasonably could be expected to cause damage to national security.
Secret	Information that the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.
Top Secret	Information that the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.

6.13.2. Task Order(s), Information Classification Levels

Authorized ordering entities should identify their information classification level requirements at the TO level.

6.14. Non-Personal Services

Authorized vendors shall only provide non-personal services under this BPA as defined under FAR Part 37.101.

No employer-employee relationship shall be implied or exist under this BPA between authorized ordering entities and authorized vendors' persons (e.g., employees, representatives, sub-contractors).

Under this BPA authorized vendors' persons shall not:

- Be placed in a position where they are under the administration, command, control, direction, evaluation, or supervision of an authorized ordering entity.
- Be placed in a position of administration, command, control, direction, evaluation, or supervision over an authorized ordering entity's persons (e.g., employees, elected officials, military personnel, political appointees).
- Be placed in a position of administration, command, control, direction, evaluation, or supervision over an authorized ordering entity's other contracted persons (e.g., employees, representatives, sub-contractors).
- Be placed in a position where they are appointed or employed by an authorized ordering entity.
- Be placed in a staff or policy making position.
- Be part of an authorized ordering entity's organization.
- Be used for the purpose of avoiding manpower ceilings or other personnel rules and regulations applicable to authorized ordering entities.
- Be used in the administration or supervision of authorized ordering entities procurement activities.

Rules, regulations, directions, and requirements that are issued by authorized ordering entities command authorities under their responsibility for administration, good order, public health, and security are applicable to all authorized vendors' persons who enter any authorized ordering entities facilities (e.g., government buildings, military installations), or who travel on authorized ordering entities transportation (e.g., aircraft, ships, vehicles). This is not to be construed or interpreted to establish any degree of authorized ordering entities control that is inconsistent with non-personal services.

6.14.1. Task Order(s), Non-Personal Services

Authorized ordering entities are authorized to identify additional non-personal services limitations and restrictions at the TO level.

6.15. On-boarding Authorized Vendors

Administrative agency Contracting Officer may on-board authorized vendors to the BPA during an established open season during the BPA ordering period for any pool or sub-pools. Any open season periods will be at the discretion of the Administrative Agency Contracting Officer.

Any contractor that meets the eligibility requirements set forth in an Open Season RFQ may submit a quotation in response to the RFQ. Any resulting awards shall incorporate the current terms and conditions as the existing BPAs, but may adjust the evaluation criteria to better respond to GSA customer needs. The BPA period of performance for Open Season awardees shall be concurrent with the existing BPA performance period of all other contractors under the vehicle. Such criteria could be determined when:

- Required by laws, regulations, or policies.
- Administrative agency determines increased capacity is required.
- Administrative agency determines increased competition is required.
- Administrative agency determines increased small business and socioeconomic participation is available or required.
- Administrative agency determines increased innovation (e.g., business, operations, security, technology) is available.

Authorized vendors shall be immediately eligible, on BPA awards resulting from open season solicitations, to submit proposals in response to BPA TO solicitations and receive TO awards with the same rights and obligations as all other BPA authorized vendors.

Contractors are hereby notified that utilization of any on-ramping procedure below does not obligate the Government to perform any other on-ramping procedure.

6.16. Off-boarding Authorized Vendors

Administrative agency Contracting Officer shall have the unilateral authority to off-board authorized vendors from the BPA, when an off-boarding event occurs during the BPA ordering period and BPA PoP.

Authorized vendors that have been off-boarded from the BPA shall not participate in any active solicitation (e.g., proposal submission, proposal evaluation) and shall have their awarded TO under the BPA terminated for cause.

Authorized vendors may be Off-ramped from the BPA under one of the following conditions:

- Debarment, Suspension, or Ineligibility as defined in FAR Subpart 9.4.
- Termination as defined in FAR Part 49.

- Contractors who fail to meet the standards of performance objectives, deliverables, or compliances. (e.g., maintaining DoD or FedRAMP authorizations)
- Taking any other action which may not be permitted or non-compliant under the BPA terms and conditions (e.g., failure to maintain certification, authorization).
- Criminal conviction, settlement, or indictment
- Failure to timely resolve / mitigate cybersecurity vulnerabilities (e.g., National Vulnerability Database)
- Failure to report cybersecurity incidents in accordance with federal regulations
- Failure to Submit Competitive Proposals 75% of the time during Single Period of Performance (PoP)

6.17. Order of Precedence

Any ambiguities or inconsistency in this BPA or awarded TO(s) shall be resolved by giving precedence[36] in the following order:

Table 9: Order of Precedence

Order of Precedence	Title
1.	U.S.C.
2.	FAR
3.	GSA, MAS
4.	GSA, MAS, Information Technology
5.	GSA, MAS, IT, SIN 518210C Cloud Computing and Cloud Related IT Professional Services
6.	ASCEND BPA
7.	ASCEND TO
8.	Authorized Vendors' Commercial SLA

6.18. Travel

The provisions affecting international air travel under this BPA shall be in accordance with *FAR 47.4 Air Transportation by U.S.-Flag Carriers*.

Travel is authorized under this BPA.

[36] Lower the number, higher the precedence (i.e., 1 is the highest).

Travel by authorized vendors, inclusive of persons (e.g., employees, representatives, sub-contractors), shall be pre-approved (i.e., in advance) by the authorized ordering entities.

6.18.1. Task Order(s), Travel

Authorized ordering entities are authorized to identify additional travel requirements at the TO level.

6.19. Travel Costs

The provisions affecting travel costs under this BPA shall be in accordance with *FAR 31.205-46 Travel Costs*.

6.19.1. Task Order(s), Travel Costs

Authorized ordering entities are authorized to identify additional travel costs requirements at the TO level.

7. General Requirement

7.1. Accounts - Cloud Service Provider

7.1.1. Access and Permissions

Authorized ordering entities are solely responsible for controlling, denying, granting, managing, and revoking user access and user permissions (e.g., read, write, execute) to the authorized ordering entities' CSP accounts (e.g., master, primary, root).

Authorized ordering entities are responsible for providing CSP accounts access and permissions to authorized vendors as required.

7.1.1.1. Task Order(s), Access and Permissions

Authorized ordering entities are authorized to identify their account access and permission requirements (e.g., personnel qualifications, approval process) at the TO level.[37]

7.1.2. Independent

Authorized ordering entities' CSP accounts (e.g., master, primary, root) shall remain individually distinct, independent, and isolated from other CSP accounts.

[37] NIST, SP 800-210: General Access Control Guidance for Cloud Systems

Authorized vendors shall not combine or commingle authorized ordering entities' CSP accounts (e.g., master, primary, root) with other accounts.

7.1.3. Linking

Authorized ordering entities are solely responsible for controlling, denying, granting, managing, and revoking the linking of CSP accounts (e.g., master, primary, root).

7.1.3.1. Task Order(s), Linking

Authorized ordering entities are authorized to identify their linking requirements (e.g., approval process) at the TO level.

7.1.4. Ownership

Authorized ordering entities CSP accounts (e.g., master, primary, root) shall be solely owned, registered to, or otherwise titled to the authorized ordering entities.

7.1.5. Portability

Authorized ordering entities' CSP accounts (e.g., master, primary, root) shall be portable (e.g., movable to another reseller) without restrictions, limitations, or operational impacts.

7.2. Banner and Consent to Monitor

Authorized vendors cloud services (i.e., IaaS, PaaS, SaaS) shall display a banner (e.g., window), as required by the authorized ordering entity, containing mandatory notice of and consent to monitoring provisions which may consist of text (i.e., letters, numbers, punctuation), graphics, and URLs (i.e., web addresses).

The banner shall be implemented and displayed post authentication (e.g., login, logon) but prior to access being granted to the cloud services.

The banner shall require affirmative / positive acceptance and agreement by designated action (e.g., click box, text entry box) prior to access being granted to the cloud services.

The banner size and content (i.e., mandatory notice of and consent to monitoring provisions) shall be customizable based on the end user device type and screen size (e.g., desktop monitor, laptop, tablets, smartphones).

7.2.1. Task Order(s), Banner and Consent to Monitor

Authorized ordering entities best practice is to identify their banner content requirements (i.e., mandatory notice of and consent to monitoring provisions) at the TO level.

7.3. Cloud Related IT Professional Services Location

Cloud related IT professional services shall be provided from and within the sovereignty and jurisdiction of the US and shall be limited to the 50 States, DC, and Territories unless the authorized ordering entity supports OCONUS operations and has an authorized exemption to this policy that supports establishment of an alternate geographic location requirement. DoD, DoS, and Intelligence Community (IC) can be authorized an exemption to the geographic location requirements and cloud related IT professional services to be performed outside the sovereignty of the US and in foreign jurisdiction(s) (e.g., military installations, embassies) in accordance with DoD, DoS, and IC applicable laws, regulations, and policies.[38, 39]

7.3.1. Task Order(s), Cloud Related IT Professional Services Location

Authorized ordering entities are responsible for identifying their cloud related IT professional services location requirements, along with any required authorized ordering entities exemption or waiver approvals, at the TO level.

7.4. Deliverables Ownership

Deliverables to authorized ordering entities, upon receipt and acceptance, shall be owned without restrictions by the authorized ordering entities.

Authorized ordering entities shall have the right to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

Acquisition sensitive deliverables (e.g., financial, administrative, cost or pricing) shall be controlled and managed in accordance with applicable laws and regulations.

Deliverables appropriately marked by authorized vendors as containing proprietary information shall be controlled and managed in accordance with applicable laws and regulations.

[38] DFARS 239.7602-2: Required storage of data within the United States or outlying areas
[39] DOS Foreign Affairs Handbook, 5 FAH-8 H-354, Cloud Computing Security

7.5. Environmental

7.5.1. Electronic Waste Recycling

Authorized vendors shall recycle their electronic waste (i.e., e-Waste) using an e-Stewards® or R2 certified electronic recycler.[40]
Electronic waste under this section shall be interpreted to be inclusive of IT equipment (e.g., laptops, printers, routers, servers, tablets), peripherals (e.g., batteries, cables, keyboards, monitors, sensors), and data center equipment (e.g., chemicals, racks, UPS, HVAC).

7.5.2. Task Order(s), Environmental

Authorized ordering entities are authorized to identify additional environmental requirements at the TO level.

7.6. Judicial or Law Enforcement Order(s)

Authorized vendors shall notify the BPA Contracting Officer, and authorized ordering entities using the authorized vendor's cloud services (i.e., IaaS, PaaS, SaaS), within 60 minutes of any judicial or law enforcement order or request (e.g., warrants, seizures, subpoenas) it receives, including those from another authorized ordering entity that could result in the loss or unauthorized disclosure of any authorized ordering entity's data. The authorized vendor shall cooperate with the authorized ordering entity(ies) to take all measures to protect the authorized ordering entity's data from any loss or unauthorized disclosure that might reasonably result from the execution of any such judicial or law enforcement order or request or similar legal process.

7.7. Key Personnel

Authorized ordering entities should identify their vendor key personnel (e.g., cloud architect) requirements at the TO level.

7.8. Logical Access

7.8.1. Logical Access Control

Authorized vendors shall restrict, monitor, and record (i.e., logical access record, logical access log) all logical access to the authorized vendors' cloud services and computing equipment leveraged in the execution of the authorized ordering entities TOs, inclusive, but not limited to the following examples:

- data storage

[40] FAR 23.7 Contracting for Environmentally Preferable Products and Services

- archive, cache, primary, secondary,
- edge computing, and networking equipment
- software code,
  - application, machine, middleware, and OS software
  - software depositories, software management systems, and software integrity systems.

7.8.1.1. Logical Access Records

The logical access record(s) (e.g., logs) shall include at a minimum:[41]

- Timestamp
- Status code for event type
- Device identifier (MAC address or other unique identifier)
- Session / Transaction ID
- Autonomous System Number
- Source IP (IPv4)
- Source IP (IPv6)
- Destination IP (IPv4)
- Destination IP (IPv6)
- Status code
- Response Code
- Response Time
- Additional headers (i.e., HTTP headers)
- Where appropriate, the username and/or userID shall be included
- Where appropriate, the command executed shall be included
- Where possible, all data shall be formatted as key-value-pairs allowing for easy extraction
- Where possible, a unique event identifier shall be included for event correlation; a unique event identifier shall be defined per event type

7.8.1.2. Logical Access Records Request

Authorized vendors shall provide logical access records on the request of an authorized ordering entity.

7.8.2. Logical Access Forensic, Inspection, Investigative

Authorized vendors shall provide authorized ordering entities immediate logical access to all the authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) computing equipment, inclusive of data storage (e.g., archive, cache, primary, secondary), edge computing, and networking equipment and software code, inclusive of application, machine, middleware,

[41] M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

and OS software, software depositories, software management systems, and software integrity systems leveraged in the execution of the authorized ordering entity's TO(s) for forensic, inspection, or investigative purposes (e.g., cybersecurity incident).

7.8.2.1. Law Enforcement Logical Access

Authorized ordering entity under this section shall be interpreted to be inclusive of the authorized ordering entity and the entities with jurisdiction for the oversight (e.g., OIG) or law enforcement (e.g., DoJ, FBI, State Police) of or for the authorized ordering entity.

7.8.2.2. Logical Isolation

Authorized vendors' cloud services computing equipment, inclusive of data storage (e.g., archive, cache, primary, secondary), edge computing, and networking equipment and software code, inclusive of application, machine, middleware, and OS software, software depositories, software management systems, and software integrity systems, may be logically isolated, but shall remain operational and functional (e.g., powered on) until the authorized ordering entity provides official guidance.

7.8.3. Logical Access - Personnel

Authorized vendors shall restrict logical access to the authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) computing equipment, inclusive of data storage (e.g., archive, cache, primary, secondary), edge computing, and networking equipment and software code, inclusive of application, machine, middleware, and OS software, software depositories, software management systems, and software integrity systems leveraged in the execution of the authorized ordering entities' TOs to US persons only.

7.9. Physical Access

7.9.1. Physical Access - Control

Authorized vendors shall restrict, monitor, and record (i.e., physical access record, physical access log) all physical access to the authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) physical computing equipment, inclusive of data storage (e.g., archive, cache, primary, secondary), edge computing, and networking equipment leveraged in the execution of the authorized ordering entities' TOs.

7.9.1.1. Physical Access Records

The physical access record(s) shall include at a minimum:

- Name
- Purpose
- Entry Date and Time

- Exit Date and Time

7.9.1.2. Physical Access Records Request

Authorized vendors shall provide physical access records on the request of an authorized ordering entity within 120 hours or defined at the TO level. In the event of a cyber incident (e.g., data breach) event, the authorized ordering entity must be provided access to log records within 72 hours.

7.9.2. Physical Access - Forensic, Inspection, Investigative

Authorized vendors shall provide the ability for the ordering entities to coordinate immediate physical access to all the authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) physical computing equipment, inclusive of data storage (e.g., archive, cache, primary, secondary), edge computing, and networking equipment leveraged in the execution of the authorized ordering entities' TOs for forensic, inspection, or investigative purposes (e.g., cybersecurity incident).

7.9.2.1. Law Enforcement Physical Access

Authorized ordering entity under this section shall be interpreted to be inclusive of the authorized ordering entity and the entities with jurisdiction for the oversight or law enforcement (e.g., DoJ, FBI, State Police) of or for the authorized ordering entity.

7.9.2.2. Physical Equipment Isolation

Authorized vendors' cloud services physical computing equipment, inclusive of data storage, edge computing, and networking equipment, may be operationally isolated, but shall remain operational and functional (e.g., powered on) until the authorized ordering entity provides official guidance.

7.9.3. Physical Access - Personnel

Authorized vendors shall restrict physical access to the authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) physical computing equipment, inclusive of data storage (e.g., archive, cache, primary, secondary), edge computing, and networking equipment leveraged in the execution of the authorized ordering entities' TOs to US persons only.

7.10. Physical Equipment Location

Authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) physical computing equipment (e.g., data center, servers), inclusive of data storage (e.g., cache, primary, secondary, archive), edge computing, and networking equipment, shall be located, provided, and maintained under and within the sovereignty and jurisdiction of the US and shall be limited to the 50 States, DC, and Territories unless the authorized ordering entity supports OCONUS operations and has an authorized exemption to this policy that supports establishment of an alternate geographic location requirement. DoD, DoS, and Intelligence

Community (IC) can be authorized an exemption (i.e., relief) to the geographic location requirements and cloud related IT professional services to be performed outside the sovereignty of the US and in foreign jurisdiction(s) (e.g., military installations, embassies) in accordance with DoD, DoS, and IC applicable laws, regulations, and policies.

Authorized vendors' physical computing equipment shall not be subject to foreign jurisdictions or foreign nations laws, regulations, or policies.

7.10.1. Task Order(s), Physical Equipment Location

Authorized ordering entities should identify their physical equipment location requirements, along with any required Agency exemption or waiver approvals, at the TO level.[42]

7.11. Registration of Services

Authorized vendors shall register cloud services (i.e., IaaS, PaaS, SaaS) in authorized ordering entities management, reporting, and tracking systems.

7.11.1. Task Order(s), Registration of Services

Authorized ordering entities are authorized to identify their registration of services requirements at the TO level.

7.12. Service Contract Reporting

Authorized vendors shall accurately and timely complete service contract reporting requirements (e.g., contractor manpower reporting).[43, 44]

7.12.1. Task Order(s), Service Contract Reporting

Authorized ordering entities should identify their service contract reporting requirements at the TO level.[45, 46, 47, 48]

7.13. Software Ownership

Authorized vendors shall not limit or otherwise restrict the ability of authorized ordering entities to access, download, or otherwise retrieve, partially or in full, the authorized ordering

[42] DFARS 239.7602-2 Required storage of data within the United States or outlying areas
[43] FAR 52.204-14 Service Contract Reporting Requirements
[44] System for Award Management (SAM), Service Contract Reporting (SCR)
[45] 10 U.S.C. 235 ARMED FORCES, Procurement of contract services: specification of amounts requested in budget
[46] 10 U.S.C. 2330a ARMED FORCES, Procurement of services: tracking of purchases
[47] DFARS 204.17 - Service Contract Inventory
[48] DFARS 204.1703 Reporting Requirements

entities software (e.g., licenses), inclusive of applications, configuration files (e.g., CaC), functions, IaC, software code, scripts, and subroutines, used by authorized ordering entities in leveraging (e.g, automate, configure, operate, use) the authorized vendor's cloud services (i.e, IaaS, PaaS, SaaS).

Authorized ordering entities' software shall always be owned by and accessible to the authorized ordering entities.

In the event open source software is utilized the Authorized vendor shall also provide the software code along with any related forked code to the authorized ordering entity.

7.14. Source Code Escrow

Authorized vendors may be required to deposit a complete copy of the authorized vendor's cloud services (i.e., IaaS, PaaS, SaaS) source code (e.g., open source software, proprietary software, software libraries) into escrow.

Escrowed source code and applicable commentary, explanations, and other documentation (i.e., escrow package), shall be accurate and complete and shall delineate and explain the structure, organization, sequencing, and operation of the source code in sufficient detail to permit an authorized ordering entity to compile, install, operate, maintain, modify, secure, and enhance the source code (i.e., cloud services).

Escrow packages, when required, shall be deposited within thirty (30) calendar days of TO awards and updated within thirty (30) calendar days of cloud services patches, updates, or upgrades.

Authorized vendors shall review and update the entire escrow package when the cloud services have a major upgrade (e.g., version 1.1 to 1.2).

Escrow packages shall be released to authorized ordering entities when:

- Source code is made publicly available (e.g., open source),
- Authorized vendors fail to timely secure (e.g., patch, update) source code,
- Authorized vendors discontinue or decommission cloud service,
- Authorized vendors are acquired by or sold to a foreign entity (e.g., business, corporation, sovereign wealth fund) or non-US citizen (i.e., foreigner),
- Authorized vendors merge with a foreign entity (e.g., business, corporation),
- Foreign entities or non-US citizens acquires an influencing stake (e.g., stock ownership, partnership, board member) in the authorized vendor
- Authorized vendors (e.g., business, corporation, owners, board members) become subject to government (e.g., US) and non-government (e.g, UN) sanctions,
- Authorized vendors cessation, for any reason, to do business (e.g., bankruptcy, insolvency, receivership),
- Authorized vendors demonstrate the inability or unwillingness to fulfill its obligations under award TO(s).

Upon release of the escrow package authorized ordering entities shall have a perpetual, irrevocable authorization to use, reproduce, prepare derivative works, update, modify, and to otherwise support the authorized ordering entities usage of the source code.

Authorized vendors shall not receive compensation for released escrow packages.

7.14.1. Task Order(s), Source Code Escrow

Authorized ordering entities are authorized to identify their source code escrow requirements at the TO level.

8. Cybersecurity Requirements

8.1. Annual Cybersecurity Assessment

Authorized vendors shall perform an annual cybersecurity assessment, conducted by a third-party cybersecurity assessor using a government (e.g., NIST SP 800-53) or commercially recognized (e.g., ISO 27001:2018) cybersecurity assessment standard, of their IS and cybersecurity practices.

The government or commercially recognized cybersecurity assessment standard used shall at a minimum evaluate and assess the authorized vendor's compliance with the requirements of *FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems.*[49, 50, 51]

8.1.1. Annual Cybersecurity Assessment Documentation

Authorized vendors shall provide the BPA administering agency with documentation of their completed annual cybersecurity assessment **[Data Deliverable]**.

The documentation shall include:

- Identification of the third-party cybersecurity assessor with corresponding contact information.
    - Identification of the cybersecurity assessment date(s).
    - A narrative summary (e.g., executive summary) of the cybersecurity assessment results (e.g., category scores) and findings (e.g., issues, risks, vulnerabilities).
    - An itemized list of any critical, high, or medium cybersecurity findings (e.g., issues, risks, vulnerabilities).

[49] NIST, SP 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
[50] NIST, SP 800-171A: Assessing Security Requirements for Controlled Unclassified Information
[51] NIST, SP 800-172: Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171

- An indicator on the status (e.g., mitigated, resolved, POA&M) for each listed critical, high, or medium cybersecurity finding (e.g., issue, risk, vulnerability).

8.1.1.1. Task Order(s), Annual Cybersecurity Assessment Documentation

Authorized ordering entities may require authorized vendors to provide their annual cybersecurity assessment documentation **[Data Deliverable]** at the TO level.

8.1.2. Annual Cybersecurity Assessment Report

Authorized vendors shall make the full and complete annual cybersecurity assessment report and findings available to the BPA Contracting Officer upon request.

8.2. Assessments and Evaluations

Authorized vendors shall allow and support authorized assessment and evaluation entities to conduct and perform, announced and unannounced, independent cybersecurity (e.g., CIA triad) and operational (e.g., performance, SLAs) assessments and evaluations of the cloud services (i.e., IaaS, PaaS, SaaS) architectures (e.g., compute, networking, storage) and security domains involved in the processing, transporting, and / or storing authorized ordering entities data.

8.2.1. Assessments and Evaluations Techniques

Authorized vendors shall allow authorized assessment and evaluation entities to use active (e.g., ethical hacker, red team, penetration testing) and passive (e.g., emulation, scanning, simulation) assessment and evaluation techniques.

8.2.1.1. Task Order(s), Assessments and Evaluations Techniques

Authorized ordering entities are authorized to identify their assessments and evaluations technique requirements at the TO level.

8.2.2. Mitigation and Remediation

Authorized vendors shall timely execute mitigation and remediation activities (e.g., fixes, patches, process improvements, updates).

Authorized vendors' failure to timely execute mitigation and remediation activities shall allow authorized ordering entities to terminate awarded TO(s).

8.2.3. Task Order(s), Assessments and Evaluations

Authorized ordering entities are authorized to identify their assessments and evaluations requirements at the TO level.

8.3. Authorization to Operate

Authorized vendors shall provide all required data, documentation, and information, inclusive of audits, diagrams, certifications, inventories, logs, manuals, metadata, photographs, procedures, reports, scans, specifications, and supply chain sourcing information, to support authorized ordering entities A&A activities and issuance of ATOs by the authorized ordering entities for the authorized vendor's cloud services (i.e., IaaS, PaaS, SaaS).

Authorized vendors shall only provide cloud services to an authorized ordering entity on the issuance and receipt of an ATO or equivalent issued by the authorized ordering entity.

ATOs are only applicable to and valid for the explicitly identified cloud services and the issuing authorized ordering entity and are non-transferable unless the authorized ordering entities have a documented reciprocity agreement.

DCAS and FedRAMP authorizations are not equivalent to or the same as an ATO and do not satisfy the ATO requirements.

8.3.1. Provisional Authority (PA)

Authorized vendors may provide limited (e.g., access, capabilities, test environment) cloud services (i.e., IaaS, PaaS, SaaS) to an authorized ordering entity under a PA or equivalent issued by the authorized ordering entity to support cloud services ATO A&A, development, pilots, testing, and / or similar activities.

8.3.2. Mitigation and Remediation

Authorized vendors shall timely execute mitigation and remediation activities (e.g., fixes, patches, process improvements, updates).

Authorized vendors' failure to timely execute mitigation and remediation activities shall allow authorized ordering entities to terminate awarded TO(s).

8.3.3. Task Order(s), Authorization to Operate

Authorized ordering entities are authorized to identify their ATO requirements at the TO level.[52, 53, 54, 55, 56]

[52] NIST, SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
[53] DoDI 8500.01: Cybersecurity
[54] DoDI 8510.01: Risk Management Framework (RMF) for DoD Information Technology (IT)
[55] DoD Cloud Computing Security Requirements Guide (DoD CC SRG)
[56] ICD 503: Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation

8.4. Cybersecurity Information and Collaboration Programs

Authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) shall actively participate in cybersecurity information and collaboration programs in support of *PPD-21: Critical Infrastructure Security and Resilience* and *PPD-41: United States Cyber Incident Coordination*.

8.4.1. United States Department of Homeland Security

Authorized vendors shall actively participate in CISA cybersecurity information and collaboration program:

- Cyber Information Sharing and Collaboration Program (CISCP)

8.4.2. United States Department of Defense

Authorized vendors shall report cybersecurity incidents to the appropriate DoD programs and service:

- Defense Industrial Base (DIB) Cybersecurity (CS) Program

8.5. Cybersecurity Technical Programs

Authorized vendors cloud services (i.e., IaaS, PaaS, SaaS) shall be compatible and interoperable with the following cybersecurity technical programs.

Authorized vendors shall not restrict, limit, or otherwise impede the functionality, operations, or performance of the following cybersecurity technical programs.

8.5.1. United States Department of Homeland Security

Authorized vendors shall be compatible and interoperable with the following DHS cybersecurity technical programs that are responsible for the monitoring, reporting, protection, and mitigation of cybersecurity threats and vulnerabilities to US Federal Government civilian agencies' IS and cloud services (i.e., IaaS, PaaS, SaaS) processing, transporting, and / or storing US Federal Government civilian agencies' data.

- CDM Program
- EINSTEIN
- TIC

8.5.2. United States Department of Defense

Authorized vendors shall be compatible and interoperable with the following DoD cybersecurity technical program that is responsible for the monitoring, reporting, protection, and mitigation of cybersecurity threats and vulnerabilities to DoD's IS and cloud services (i.e., IaaS, PaaS, SaaS) processing, transporting, and / or storing DoD's data.

- CMMC v2.0 (based on program applicability)

8.5.3. Task Order(s), Cybersecurity Program Requirements

Authorized ordering entities are authorized to identify additional cybersecurity program requirements at the TO level.

8.6. Incident Investigations

Authorized vendors shall fully comply with and support all cybersecurity incident investigations, associated with providing cloud services (i.e., IaaS, PaaS, SaaS) or cloud-related IT professional services, to authorized ordering entities.

8.6.1. Incident Investigations Restrictions or Limitations

Authorized vendors shall not have or enter into any (e.g., government, commercial) agreements or contractual relationships that limits or restricts the authorized vendor from fully complying and supporting cybersecurity incident investigations by an authorized ordering entity.[57]

8.6.1.1. Law Enforcement

Authorized ordering entity under this section shall be interpreted to be inclusive of the authorized ordering entity and the entity(ies) with jurisdiction for the oversight (e.g., OIG) or law enforcement (e.g., DoJ, FBI, State Police) of or for the authorized ordering entity.

8.6.2. Task Order(s), Incident Investigations Restrictions or Limitations Requirements

Authorized ordering entities shall not include requirements, at the TO level, that would restrict or limit an authorized vendor from fully complying and supporting cybersecurity incident investigations.[58]

8.7. Incident Reporting

Authorized vendors providing cloud services (i.e., IaaS, PaaS, SaaS) shall actively participate in cybersecurity incident reporting programs in support of *Presidential Policy Directive (PPD)-21: Critical Infrastructure Security and Resilience* and *PPD-41: United States Cyber Incident Coordination*.

Authorized vendors shall report cybersecurity incidents (e.g., attacks, ransomware), associated with providing cloud services (i.e., IaaS, PaaS, SaaS) or cloud-related IT professional services to the BPA Contracting Officer and the impacted authorized ordering

[57] Executive Order 14028: Improving the Nation's Cybersecurity
[58] Executive Order 14028: Improving the Nation's Cybersecurity

entity or entities in a timely manner consistent with Presidential Executive Orders[59] and GSA IT policy requirements.[60]

8.7.1. United States Department of Homeland Security

Authorized vendors shall report cybersecurity incidents (e.g., attacks, ransomware) to the appropriate DHS, CISA, United States Computer Emergency Readiness Team (US-CERT) programs and services:

- AMAC Malware Analysis Submissions
- Coordinated Vulnerability Disclosure (CVD) Program
- Cyber Threat Indicator and Defensive Measure Submission System
- Incident Reporting System

Authorized vendors shall timely report cybersecurity incidents to CISA/US-CERT within the following time periods:

- Cyberattack within 72 hours
- Ransomware payment within 24 hours

8.7.2. United States Department of Defense

Authorized vendors shall report cybersecurity incidents to the appropriate DoD programs and service:

- DoD Defense Industrial Base (DIB) Cyber Reports

Authorized vendors shall timely report cybersecurity incidents (e.g., attacks, ransomware), associated with providing cloud services (i.e., IaaS, PaaS, SaaS) for NSS, Defense Business Systems, etc., in accordance with CJCSM 6510.01B, *Cyber Incident Handling Program, July 10, 2012 (Amended December 18, 2014)*

Authorized vendors shall report the following cybersecurity incidents to the Defense Industrial Base Collaborative Information Sharing Environment (DCISE) within the following time periods:

- Cyberattack within 72 hours
- Ransomware payment within 24 hours

8.7.3. Task Order(s), Incident Reporting Program Requirements

Authorized ordering entities should identify additional cybersecurity incident reporting program requirements at the TO level.

[59] Executive Order 14028: Improving the Nation's Cybersecurity
[60] IT Security Procedural Guide: Incident Response (IR) CIO-IT Security-01-02

Authorized ordering entities are responsible for identifying the person(s), office(s) (e.g., SOC), organization(s), or other cybersecurity entities that cybersecurity incidents are to be timely reported to at the TO level.

Authorized ordering entities are responsible for identifying at the TO level the means (e.g., email, hotline) and the corresponding information (e.g., email address, telephone number) for cybersecurity incident reporting.

8.7.4. Incident Reporting Restrictions or Limitations

Authorized vendors shall not have or enter into any (e.g., government, commercial) agreements or contractual relationships that limits or restricts the authorized vendor from timely reporting cybersecurity incidents to an authorized ordering entity.[61]

8.7.4.1. Law Enforcement

Authorized ordering entity under this section shall be interpreted to be inclusive of the authorized ordering entity and the entities with jurisdiction for the oversight or law enforcement (e.g., DoJ, FBI, State Police) of or for the authorized ordering entity.

8.7.5. Task Order(s), Incident Reporting Restrictions or Limitations Requirements

Authorized ordering entities shall not include requirements, at the TO level, that would restrict or limit an authorized vendor from timely reporting cybersecurity incidents.[62]

8.8. Incident Response

Authorized vendors shall develop and maintain an internal Cybersecurity Incident Response Plan in accordance with NIST SP 800-61 (current revision) guidelines and in support of the DHS National Cyber Incident Response Plan strategic framework.

8.9. Information Assurance Vulnerability Management (IAVM)

Authorized vendors shall monitor US-CERT issued Information Assurance Vulnerability Assessment (IAVA) (e.g., alerts, bulletins, technical advisories) for IAVA(s) that impact authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS).

[61] Executive Order 14028: Improving the Nation's Cybersecurity
[62] Executive Order 14028: Improving the Nation's Cybersecurity

Authorized vendors shall monitor NIST National Vulnerabilities Database (NVD) and / or Common Vulnerabilities and Exposures (CVE)(R) records for vulnerabilities that impact authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS).

Authorized vendors shall monitor other appropriate services (e.g., academic, commercial, government) for vulnerabilities that impact authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS).

Authorized vendors shall timely manage (e.g., IAVM) and execute mitigation and remediation activities (e.g., fixes, patches, updates) in response to IAVA(s), NVD and CVE(R) records, and other services announcements.

Authorized vendors' failure to execute timely mitigation and remediation activities shall allow:

- BPA Contracting Officer to terminate authorized vendors' BPA award(s).
- Authorized ordering entities to terminate awarded TO(s).

8.10. Multi-Factor Authentication

8.10.1. Cloud Service Provider Accounts

Access (i.e., authentication and authorization) to CSP accounts (e.g., master, primary, root) shall be executed by phishing-resistant MFA solutions[63, 64, 65, 66, 67, 68] (e.g., Derived PIV,[69] PIV,[70] Biometrics,[71] Web Authentication[72]).

8.10.1.1. Reauthentication and Reauthorization

Access reauthentication and reauthorization shall be required every 12 hours or less regardless of activity.[73]

Access reauthentication and reauthorization shall be required following any period of inactivity lasting 15 minutes or longer.[74]

[63] NIST, SP 800-63-3: Digital Identity Guidelines
[64] NIST, SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing
[65] NIST, SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management
[66] NIST, SP 800-63C: Digital Identity Guidelines: Federation and Assertions
[67] Executive Order 14028: Improving the Nation's Cybersecurity
[68] M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
[69] NIST SP 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials
[70] FIPS PUB 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors
[71] NIST SP 800-76: Biometric Specifications for Personal Identity Verification
[72] Web Authentication (WebAuthn)
[73] NIST, SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management
[74] NIST, SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management

8.10.2. Cloud Services

Access to cloud services (i.e., IaaS, PaaS, SaaS), that require user login (i.e., authentication and authorization), shall be executed by phishing-resistant MFA solutions[75, 76, 77, 78, 79, 80] (e.g., Derived PIV,[81] PIV,[82] Biometrics,[83] Web Authentication[84]).

8.10.2.1. Reauthentication and Reauthorization

Access reauthentication and reauthorization shall be required every 12 hours or less regardless of activity.[85]

Access reauthentication and reauthorization shall be required following any period of inactivity lasting 15 minutes or longer or when a change to endpoint IP is detected (i.e., changing hotspot or connecting/disconnecting from VPN).[86]

8.10.3. Task Order(s), Multi-Factor Authentication

Authorized ordering entities are authorized to identify MFA requirements at the TO level.

8.11. Customer-based Testing

Authorized vendors shall allow authorized ordering entities to conduct and perform cybersecurity (e.g., CIA triad) and operational (e.g., performance, SLAs) testing of the authorized ordering entities' solutions (e.g., applications, configurations, databases, services, software, websites) deployed and operating within the cloud services (i.e., IaaS, PaaS, SaaS) processing, transporting, and / or storing authorized ordering entities data.

8.12. Customer-based Testing Techniques

Authorized vendors shall allow authorized ordering entities to use active (e.g., ethical hacker, red team, penetration testing) and passive (e.g., emulation, scanning, simulation) testing techniques in support of their vulnerability assessment program.

[75] NIST, SP 800-63-3: Digital Identity Guidelines
[76] NIST, SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing
[77] NIST, SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management
[78] NIST, SP 800-63C: Digital Identity Guidelines: Federation and Assertions
[79] Executive Order 14028: Improving the Nation's Cybersecurity
[80] M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
[81] NIST SP 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials
[82] FIPS PUB 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors
[83] NIST SP 800-76: Biometric Specifications for Personal Identity Verification
[84] Web Authentication (WebAuthn)
[85] NIST, SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management
[86] NIST, SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management

8.12.1. Task Order(s), Customer Testing Techniques and Requirements

Authorized ordering entities are authorized to identify their testing techniques and requirements at the TO level.

8.13. Training

Authorized vendors' persons (e.g., employees, representatives, sub-contractors) shall provide documentation of successful completion of authorized ordering entities annual cybersecurity training and certification requirements. Training programs should be based upon NIST SP 800-181 Rev1, *Workforce Framework for Cybersecurity (NICE Framework)* and NIST Interagency Report (NISTIR) 8355, *NICE Framework Competencies: Assessing Learners for Cybersecurity Work*. **[Deliverable X]**

8.13.1. Task Order(s), Training

Authorized ordering entities are responsible for identifying cybersecurity training and certification requirements at the TO level.

9. Data Requirements

9.1. Data Access

Authorized vendors shall not limit or otherwise restrict the ability of authorized ordering entities to access, download, or otherwise retrieve, partially or in full, the authorized ordering entity's data from the authorized vendor’s cloud services (i.e., IaaS, PaaS, SaaS).

9.2. Data Access Control

All access to authorized ordering entities’ and authorized vendors’ cloud services data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s), shall be restricted, monitored, and recorded (i.e., access record).

9.2.1. Data Access Records

The access record(s) shall include at a minimum:

- Device Name
- Device IP Address
- Device MAC Address
- Data Access Date and Time
- Data Exit Date and Time

- Data Action (e.g., read, write, modify)

9.2.2. Data Access Records Request

Authorized vendors shall provide data access record(s) on the request of an authorized ordering entity.

9.3. Data Access Forensic, Inspection, Investigative

Authorized ordering entities shall have immediate logical access to all the authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s), for forensic, inspection, or investigative purposes (e.g., cybersecurity incident).[87, 88]

9.3.1. Law Enforcement Data Access

Authorized ordering entity under this section shall be interpreted to be inclusive of the authorized ordering entity and the entity(ies) with jurisdiction for the oversight (e.g., OIG) or law enforcement (e.g., DoJ, FBI, State Police) of or for the authorized ordering entity.

9.3.2. Data Isolation

If authorized ordering entities' data, inclusive of derivative data, metadata, and log(s) are co-located with non-authorized ordering entities' data, inclusive of derivative data, metadata, and log(s), the authorized ordering entities' data shall be isolated into a secure space (e.g., physical, virtual) to support the investigative process and all the data to where it shall be accessed, reviewed, scanned, or forensically evaluated by the authorized ordering entities.

9.3.2.1. Original Data

All original (e.g., unaltered, unedited) data, inclusive of derivative data, metadata, and log(s), shall be maintained (e.g., snapshot) to support forensic evaluation.

9.4. Data Access - Personnel

Authorized vendors shall restrict data access to authorized ordering entities' and authorized vendors' cloud services data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s) to US persons only.

[87] Executive Order 14028: Improving the Nation's Cybersecurity

[88] M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

9.5. Data Access, Use, Disclosure

Authorized vendors, inclusive of persons (e.g., employees, representatives, sub-contractors), shall not access, use, or disclose privately, commercially (e.g., 3rd parties), or publicly the authorized ordering entities' data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s), unless specifically authorized by the terms of the authorized ordering entities awarded TO(s).

9.5.1. Anonymized Data Access, Use, Disclosure

Authorized vendors, inclusive of persons (e.g., employees, representatives, sub-contractors), shall not access, use, or disclose privately, commercially (e.g., 3rd parties), or publicly any anonymized data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s), unless specifically authorized by the terms of the authorized ordering entities awarded TO(s).

9.5.2. Unauthorized Data Access, Use, Disclosure Liabilities

Unauthorized data access, use, or disclosure may subject the authorized vendor, inclusive of persons (e.g., employees, representatives, sub-contractors), to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by unauthorized data access, use, or disclosure.

9.6. Data At Rest Protection (DARP)

Authorized vendors shall implement, provide, and support DARP solutions (e.g., encryption) in their cloud services (i.e., IaaS, PaaS, SaaS) for authorized ordering entity's data at rest (e.g., archives, backups, databases, storage).[89, 90]

Authorized vendors provided DARP solutions shall allow authorized ordering entities to establish or provide their own encryption keys.

9.6.1. Task Order(s), Data At Rest Protection

Authorized ordering entities are authorized to identify DARP requirements at the TO level.

[89] Executive Order 14028: Improving the Nation's Cybersecurity
[90] M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

9.7. Data Encryption

Authorized vendors shall implement, provide, and support FIPS PUB 197: Advanced Encryption Standard (AES) data encryption solutions and third-party key management services in their cloud services (i.e., IaaS, PaaS, SaaS).[91]

Authorized vendors' provided data encryption solutions shall allow authorized ordering entities to establish or provide their own encryption keys.

9.7.1. Task Orders, Data Encryption

Authorized ordering entities are authorized to identify data encryption requirements at the TO level.

9.8. Data Format

Authorized vendors shall not convert or otherwise change or digitally manipulate the authorized ordering entities' data format (e.g., file type) to another or proprietary data format without the authorization of the authorized ordering entities.

Authorized vendors shall provide the capability to revert / reconvert the authorized ordering entities' data format (e.g., file type) to the original (e.g., MPEG-2) or newest version of the data format (e.g., MPEG-4).

Authorized vendors shall provide the capability to convert all authorized vendors' proprietary data format(s) to non-proprietary, commercially available, and standardized data format(s) (e.g., CSV, JPEG, MPEG, XML).

9.8.1. Task Order(s), Data Format

Authorized ordering entities are authorized to identify additional data format requirements at the TO level.

9.9. Data Location

Authorized ordering entities' data, inclusive of derivative data, metadata, and logs generated in the execution of the authorized ordering entities' TO(s), shall only be processed (e.g., compute), cached, stored (e.g., primary, secondary), or archived within the sovereignty and jurisdiction of the US and shall be limited to the 50 States, DC, and Territories unless the authorized ordering entity supports OCONUS operations and has an authorized exemption to this policy that supports establishment of an alternate geographic location requirement. DoD, DoS, and Intelligence Community (IC) (i.e., certain authorized ordering entities) can be

[91] NIST SP 800-175B Rev 1: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

authorized an exemption (i.e., relief) to the geographic location requirements and cloud related IT professional services to be performed outside the sovereignty of the US and in foreign jurisdiction(s) (e.g., military installations, embassies) in accordance with DoD, DoS, and IC applicable laws, regulations, and policies.[92, 93]

Authorized ordering entities' data shall not be subject to foreign jurisdictions or foreign nations laws, regulations, or policies.

Authorized vendors' data, inclusive of administrative data, support data, and billing data, generated in the execution of the authorized ordering entities' TO(s), shall only be processed (e.g., compute), cached, stored (e.g., primary, secondary), or archived within the sovereignty and jurisdiction of the US and shall be limited to the 50 States, DC, and Territories.

Authorized vendors' data shall not be subject to foreign jurisdictions or foreign nations laws, regulations, or policies.

9.9.1. Task Order(s), Data Location

Authorized ordering entities shall identify their data location requirements[94], along with any required Agency exemption or waiver approvals, at the TO level.

9.10. Data Mining, Scanning

Authorized vendors, inclusive of persons (e.g., employees, representatives, sub-contractors), shall not data mine, scan, or otherwise interrogate, investigate, or analyze via manual or automated means authorized ordering entities' data. This prohibition is inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s), unless specifically authorized by the terms of this BPA or the authorized ordering entities awarded TO(s).

9.10.1. Operations and Maintenance, Cybersecurity, Performance

Authorized vendors, inclusive of persons, are authorized in full or in partial to scan or otherwise interrogate, investigate, or analyze manually or automated authorized ordering entities' data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s), in the performance of O&M activities, cybersecurity activities (e.g., antivirus / malware detection, cybersecurity incident response), or performance improvement activities.

[92] DFARS 239.7602-2: Required storage of data within the United States or outlying areas
[93] DOS Foreign Affairs Handbook, 5 FAH-8 H-354, Cloud Computing Security
[94] DFARS 239.7602-2 Required storage of data within the United States or outlying areas

9.11. Data Ownership

Authorized ordering entities shall maintain sole ownership rights of all authorized ordering entities' data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s).

Authorized vendors shall have no ownership rights to authorized ordering entities' data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s).

9.12. Data Quarantine, Isolation, Restricted Access

Authorized vendors, inclusive of persons (e.g., employees, representatives, sub-contractors), are authorized to quarantine, isolate, or otherwise restrict access to any authorized ordering entities' data that is found or suspected to be compromised or infected with a cybersecurity vulnerability (e.g., virus, worm, ransomware, malware).

9.12.1. Cybersecurity Vulnerability Notification

Authorized vendors shall notify the authorized ordering entities of any authorized ordering entities' data that is found or suspected to be compromised or infected with a cybersecurity vulnerability and coordinate the appropriate cybersecurity incident response to mitigate and resolve.

9.12.2. Data Deletion, Destruction

Authorized vendors, inclusive of persons, shall not delete nor otherwise destroy the authorized ordering entities' data that is found or suspected to be compromised or infected with a cybersecurity vulnerability.

9.13. Data Rights

The provisions affecting data rights under this BPA shall be in accordance with *FAR 52.227-14 Rights in Data-General*.

Authorized ordering entities shall have unlimited data and metadata rights to all authorized ordering entities' data provided to, created, developed in, loaded, processed by, transitioned to, or hosted by authorized vendors in the execution of the authorized ordering entities awarded TO(s).

Authorized ordering entities shall have unlimited data rights to all authorized ordering entities' developed software, inclusive of applications, configuration files (e.g., CaC), functions, IaC, software code, scripts, and subroutines, used by authorized ordering entities

in leveraging (e.g., automate, configure, operate, use) the authorized vendors cloud services (i.e., IaaS, PaaS, SaaS).

9.13.1. Derived Data

Authorized ordering entities shall have unlimited data rights to all authorized vendors' derived data, from the authorized ordering entities data, to include analytics, logs, metadata, scans, etc. generated in the execution of the authorized ordering entities awarded TO(s).[95]

Authorized ordering entities shall have the unlimited rights to request and shall receive from authorized vendors complete copies of authorized vendors' derived data.

9.13.2. Task Order(s), Data Rights

Authorized ordering entities are authorized to identify additional data rights requirements[96, 97, 98] at the TO level

9.14. Data Spillage

Authorized ordering entities' data, inclusive of derivative data, metadata, and log(s) generated in the execution of the authorized ordering entities' TO(s), shall be contained, maintained, and restricted to the data's designated security boundary (e.g., FedRAMP Moderate, FedRAMP High, DoD IL 2, DoD IL 6).

Authorized vendors shall immediately notify authorized ordering entities on identification that the authorized ordering entities' data has spilled from one security boundary to another security boundary (i.e., spillage) without authorization. Authorized vendors shall follow the authorized ordering entities' instructions to mitigate (e.g., clean, sanitize) the spillage.

9.14.1. Task Order(s), Data Spillage Reporting Information

Authorized ordering entities shall identify the person(s), office(s) (e.g., SOC), organization(s), or other entities that spillages are to be immediately reported to at the TO level.

Authorized ordering entities shall identify at the TO level the means (e.g., email, hotline) and the corresponding information (e.g., email address, telephone number) for spillage reporting.

[95] M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents
[96] DFARS 252.227-7013 Rights in Technical Data—Noncommercial Items
[97] DFARS 252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation
[98] DFARS 252.227-7015 Technical Data–Commercial Items

9.15. Data Sanitization

Authorized vendors shall maintain and ensure the confidentiality of authorized ordering entities data by preventing unauthorized access, disclosure, or retrieval.[99]

9.15.1. Data Deletion

Authorized vendors shall sanitize data from cloud services (i.e., IaaS, PaaS, SaaS) data storage devices (e.g., cache, primary and secondary storage, backups, archives), by nondestructive (e.g., cryptographic erase, overwrite) means based on the authorized ordering entity's requirements for the information classification level[100], when authorized ordering entities delete their data or when authorized ordering entities terminate their usage of authorized vendors' cloud services.

9.15.2. Data Storage Device Removal

Authorized vendors shall sanitize data from cloud services (i.e., IaaS, PaaS, SaaS) data storage devices, by nondestructive (e.g., cryptographic erase, overwrite) means based on the information classification level, when authorized vendors remove computer readable medium from operational usage and maintain full access and asset control.

9.15.3. Data Storage Device Decommission and Disposal

Authorized vendors shall sanitize data from cloud services (i.e., IaaS, PaaS, SaaS) data storage devices, by destructive (e.g., degaussing, grinding, shredding) and nondestructive (e.g., cryptographic erase, overwrite) means based on the information classification level, when authorized vendors decommission or dispose of their computer readable medium.

9.15.4. Task Order(s), Data Sanitization

Authorized ordering entities are authorized to identify data sanitization requirements at the TO level.

9.16. Data Transceiving Caching

Authorized vendors may temporarily cache authorized ordering entities' data outside the sovereignty and jurisdiction of the US when actively transceiving (e.g., transport, routing) authorized ordering entities' encrypted (e.g., DARP, HTTPS, TLS) data to or from an authorized source or an authorized destination that is outside the sovereignty and jurisdiction of the US.

[99] NIST, SP 800-88 Rev. 1: Guidelines for Media Sanitization
[100] Executive Order 12829: National Industrial Security Program

9.16.1. Task Order(s), Data Transceiving Caching Requirements

Authorized ordering entities are authorized to identify additional data transceiving caching security requirements (e.g., encryption, policies, prohibitions, protocols, routing) at the TO level.

9.17. Data Transceiving Protection

Authorized vendors shall implement, provide, and support data transceiving (e.g., transport, routing) protection solutions (e.g., encryption, policies, protocols, secure communications, routing) in their cloud services (i.e., IaaS, PaaS, SaaS) for authorized ordering entities' data.[101]

Data transceiving protection solutions shall be implemented, provided, and supported for both internal (e.g., within the CSP security boundary, Intranet) and external (e.g., outside the CSP security boundary, Internet) data transceiving.

9.17.1. Task Order(s), Data Transceiving Protection Requirements

Authorized ordering entities are authorized to identify data transceiving protection requirements (e.g., internal, external) at the TO level.

10. Authorized Ordering Entity Requirements

All authorized ordering entities that use this BPA in the execution of any TO shall comply with the following requirements unless otherwise granted a waiver from the BPA administering agency.

10.1. Accounts Management

10.1.1. Account Requests

Authorized ordering entities shall process authorized vendor account requests in accordance with the authorized ordering entities' review and approval processes.

Authorized ordering entities shall configure approved accounts with the appropriate access and permissions.

[101] Executive Order 14028: Improving the Nation's Cybersecurity

10.1.2. Account Change Requests

Authorized ordering entities shall process authorized vendor account change requests (e.g., new accounts, account deletions) in accordance with the authorized ordering entities' review and approval processes.

Authorized ordering entities shall configure approved account changes with the appropriate access and permissions.

10.1.3. Accounts - Cloud Service Provider(s)

10.1.3.1. Existing Accounts

Authorized ordering entities shall provide existing CSP account information to the authorized vendors and coordinate with the authorized vendors in transferring existing CSP accounts.

10.1.3.2. New Accounts

Authorized ordering entities shall provide required CSP account information to the authorized vendors and coordinate with the authorized vendors in creating CSP accounts.

10.2. Post Award Management

10.2.1. Exercise of Option Period of Performance (PoP) Notifications

Authorized ordering entities shall provide written notification to authorized vendors at least 30 calendar days prior to the exercise of an option PoP.[102]

Authorized ordering entities shall notify the BPA Contracting Officer within <<FILL IN>> days of the exercise of an option PoP.

10.2.2. Invoicing

10.2.2.1. Task Order(s) Invoice Submission Cover Sheet

Authorized ordering entities shall identify their TO(s) invoice cover sheet requirements (e.g., CLIN summary, utilization discounts balance, LOAs) and submission requirements (e.g., systems, payments) at the TO level.

[102] FAR 17.207 Exercise of Options

10.2.2.2. Task Order(s) Invoice Approval

Authorized ordering entities shall receive, review, approve, and timely pay authorized vendors invoices.

10.2.3. Networking and Routing

Authorized ordering entities shall coordinate with and provide authorized vendors with required networking (e.g., MAC addresses) and routing configuration information (e.g., IP addresses) to allow authorized vendors to configure authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) connectivity (e.g., firewalls, MTIPS, TIC) in accordance with awarded TO requirements.

10.2.4. Travel

10.2.4.1. Task Order(s) Travel Requests

Authorized ordering entities shall identify their TO(s) travel requests requirements (e.g., timeframe, format, information) at the TO level.

10.2.4.2. Task Order(s) Travel Approvals

Authorized ordering entities shall receive, review, and timely approve authorized vendors travel requests.

10.2.4.3. Task Order(s) Travel Documentation

Authorized ordering entities shall provide authorized vendors with any required supporting documentation needed in obtaining necessary travel documents.

11. Authorized Vendor Requirements

All authorized vendors that use this BPA in the execution of any TO shall comply with the following requirements unless otherwise granted a waiver from the BPA administering agency.

11.1. Blanket Purchase Agreement Training

11.1.1. Federal Contracts Administrator

Authorized vendors shall complete all required BPA Contracting Officer's training prior to submission of TO proposal.

11.2. Pre-Award

11.2.1. Service Catalog

Authorized vendors shall maintain an accurate, complete, and up to date service capabilities catalog that identifies authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS) and / or the cloud-related IT professional services that the authorized vendor is authorized to offer, negotiate, and sell under this BPA.

11.2.1.1. Service Catalog Audit Corrective Actions

Authorized vendors shall resolve all negative findings (e.g., deficiencies, discrepancies, errors) and complete required corrective actions within 1 month of administrative notification.

11.2.1.2. Service Catalog Authorized Services

Authorized vendors service catalogs shall only include the cloud services and / or the cloud-related IT professional services that authorized vendors have been authorized to provide in accordance with authorized vendors BPA award(s) (i.e., pools, sub-pools).

11.2.1.3. Service Catalog Review and Attestation

Authorized vendors shall review and attest once every 6 months per BPA ordering period that their service catalogs are accurate, complete, and up to date.

11.2.1.4. Service Catalog, Cloud Services

11.2.1.4.1. Data Elements

Authorized vendors cloud services catalogs shall include the required data elements and may include the optional data elements. (Reference Appendix D)

1673

Table 10: Service Catalog Required Data Elements			
Data Element	Format	Examples / **[Valid Values]**	Notes
BPA Pool and Sub-Pool Number	Text	1-1, 2-1	
TO PoP	Numerical	00, 01, 02, 03	
TO PoP Start Date	YYYY MM DD	2022 01 01	
TO PoP End Date	YYYY MM DD	2022 12 31	
CSP Name	Text	Cloud Inc.	
Service Name	Text	General Compute Large Server	
Service Description	Text	Server, 4 vCPU, 64 GB RAM, 25 Gbps	
Service Model	Text	**[IaaS, PaaS, SaaS]**	
Authorizing Entity	Text	**[DoD, FedRAMP]**	If a cloud service has multiple authorizing entities the cloud service shall have an entry in the catalog for each applicable authorizing entity (i.e., DoD, FedRAMP) with associated authorizing entity's authorization data.
Impact Level	Text	**[LI-SaaS, Low, Moderate, High, 2, 4, 5, 6]**	

Authorization Date	YYYY MM DD	2021 07 04	
Discontinuation Date	YYYY MM DD	2025 12 25	Identifies the actual or planned discontinuation, decommissioning, or sunset date for a cloud service. If no "Discontinuation Date" has been established a value of "Null" shall be entered.
CSP Identifier	Text, Numerical, Alphanumeric	ABCDEFGHI, 1234567890, A1B2C3D4E5F6	Identifies the CSP's unique code (e.g., UPC) for each cloud service and is universal across resellers. The "CSP Identifier" should also be universal across commercial and non-commercial (e.g., government) customers.
Effective Price Date	YYYY MM DD	2022 02 15	
Service Price	Currency	$5.4321	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the price for a quantity of one (1) (i.e., unit price) for the cloud service in US currency (i.e., US dollars) out to four (4) decimal places (i.e., ten-thousandths).
Unit of Measure	Text	Compute per Hour, GB, Subscription, Transaction	
EPEAT™ Registered	Text	**[Yes, No]**	Identifies if the cloud service operates on EPEAT™ Registered equipment (e.g., computers, networking, servers).
ENERGY STAR® Certified	Text	**[Yes, No]**	Identifies if the cloud service operates on ENERGY STAR® Certified equipment (e.g., servers, storage, networking equipment).

1674

Table 11: Service Catalog Optional Data Elements			
Data Element	Format	Examples / **[Valid Values]**	Notes
SKU	Text, Numerical, Alphanumeric	ABCDEFGHI, 1234567890, A1B2C3D4E5F6	Is any text, numerical, or alphanumeric indicator that an authorized vendor uses to identify, track, and manage their cloud services internally.
ZTA Pillar	Text	**[Application, Data, Device, Infrastructure, Orchestration and Automation, Network, User, Visibility and Analytics]**	1. The "GSA Zero Trust Architecture (ZTA) Buyer's Guide" defines eight (8) foundational pillars of ZTA and the core components of each pillar. 2. The completion of the ZTA Pillar and ZTA Component data elements will assist authorized ordering entities in identifying cloud services that provide specific capabilities and functions
ZTA Component	Text	*Application* **[Application Security, Any Device Access, Container Security, Isolation, Secure Access Cloud, Web Application Firewall]** *Data* **[Classification, Data Loss Prevention, Data Security, Encryption, Industry Compliance, Integrity]** *Device* **[Device Authentication, Device Compliance, Device Identity, Device Inventory, Device Management, Device Security, Enterprise Mobility Management, Vulnerability Management]** *Infrastructure* **[Cloud Access Security Broker, Cloud Workload Protection, SaaS Management Platform, Secure Access Service Edge]**	1. The "GSA Zero Trust Architecture (ZTA) Buyer's Guide" defines eight (8) foundational pillars of ZTA and the core components of each pillar. 2. The completion of the ZTA Pillar and ZTA Component data elements will assist authorized ordering entities in identifying cloud services that provide specific capabilities and functions. 3. The valid values for the ZTA Component are determined by the selected ZTA Pillar.

		Orchestration and Automation **[Policy Administrator (PA), Policy Enforcement Point (PEP), Policy Engine (PE), Security Policy Management]** *Network* **[Network Access Control, Network Security, Segmentation, Session Protection, Software-Defined Networking, Transport Encryption, Zero Trust Architecture, Zero Trust Network Access]** *User* **[Access Management, Authentication, Dynamic Risk Scoring, Conditional Access, Identity Management, User and Event Behavior Analytics]** *Visibility and Analytics* **[Continuous Diagnostics and Mitigation (CDM) System, Device Visibility, Threat Intelligence, Security Information and Event Management (SIEM)]**	

1675

11.2.1.5. Service Catalog, Cloud-Related IT Professional Services

11.2.1.5.1. Required Data Elements

Authorized vendors cloud-related IT professional services catalogs shall include the required data elements and may include the optional data elements. (Reference Appendix E)

Table 12: Service Catalog, Cloud Related IT Professional Services Required Data Elements

Data Element	Format	Examples / **[Valid Values]**	Notes
BPA Pool and Sub-Pool Number	Text	3-1, 3-2	
TO PoP	Numerical	00, 01, 02, 03	
TO PoP Start Date	YYYY MM DD	2022 01 01	
TO PoP End Date	YYYY MM DD	2022 12 31	
Professional Service	Text	Cybersecurity Forensics	
Professional Service Description	Text	Services involved with processing, preserving, and analyzing computer-related evidence.	
Clearance Level	Text	**[Tier 1 (T1) Non-Sensitive Positions - Low Risk, Tier 2 (T2) Non-Sensitive Public Trust Positions - Moderate Risk, Tier 4 (T4)**	If a cloud related IT professional service has multiple clearance levels the cloud related IT professional service shall have an entry in the

		Non-Sensitive Public Trust Positions - High Risk, Tier 3 (T3) National Security Positions - Secret / Confidential Clearance, Tier 5 (T5) National Security Positions - Top Secret Clearance]	catalog for each applicable clearance level (i.e., Tier 4 (T4) Non-Sensitive Public Trust Positions - High Risk, Tier 3 (T3) National Security Positions - Secret / Confidential Clearance).
Geographical Location	Text	**[CONUS, GSA Region 1 New England, GSA Region 2 Northeast and Caribbean, Region 3 Mid-Atlantic, GSA Region 4 Southeast Sunbelt, GSA Region 5 Great Lakes, GSA Region 6 The Heartland, GSA Region 7 Greater Southwest, GSA Region 8 Rocky Mountain, GSA Region 9 Pacific Rim GSA Region 10, Northeast Arctic, GSA Region 11 National Capital, OCONUS]**	1. The authorized vendor shall identify at least one labor rate and geographic location per cloud related IT professional service. 2. The authorized vendor may identify multiple geographic locations per cloud related IT professional service. 3. The authorized vendor's identified geographic location(s) shall represent the authorized vendor's maximum area of business operations. 4. The authorized vendor may identify different labor rates per geographic location. 5. If an authorized vendor has multiple geographic locations the cloud related IT professional service shall have a separate entry in the catalog for each geographic location.
Place of Performance	Text	**[Authorized Ordering Entity, Authorized Vendor, Remote]**	If a cloud related IT professional service has multiple places of performance the cloud related IT professional service shall have an entry in the catalog for each applicable place of performance (i.e., authorized ordering entity, authorized vendor, remote).

Cloud Related IT Professional Service Code	Text, Numerical, Alphanumeric	ABCDEFGHI, 1234567890, A1B2C3D4E5F6	The authorized vendor will receive the "Cloud Related IT Professional Service Code" from the administrative agency.
Effective Price Date	YYYY MM DD	2022 02 15	
Service Price	Currency	$125.25	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the price for the cloud related IT professional service in US currency (i.e., US dollars) out to two (2) decimal places (i.e., hundredths).
Unit of Measure	Text	Hourly Rate	

1680

11.2.1.6. Service Catalog Format

Authorized vendors shall provide service catalogs in the required format provided by the BPA Administering agency. (Sample References: Appendix D & E)

Service catalogs shall be provided in spreadsheet machine readable format, unlocked, and not password protected. All spreadsheet data shall be contained in the appropriate spreadsheet cells with the correct data type (e.g., number, text). The spreadsheet shall not contain any embedded images or other graphics.

11.2.1.6.1. Common Catalog Platform

RESERVED

During the ordering period of this BPA, it is projected that the GSA Common Catalog Platform (CCP) will become operational. The BPA administering agency shall provide guidance, instructions, and manage the transition of service catalogs under this BPA to the GSA CCP at such future time.

11.3. Task Order Solicitations

11.3.1. No-Bid Notification(s)

Authorized vendors shall notify the BPA Contracting Officer within X days of the TO solicitation closing date when an authorized vendor decides not to submit a proposal (i.e., No-Bid). The notification shall include the following information:

- Solicitation Number
- Solicitation Closing Date
- Contextual explanation for not submitting a proposal (i.e., No-Bid)

11.3.1.1. Sole Source and Brand Name Solicitation(s)

Authorized vendors are not required to notify the BPA Contracting Officer of a no-bid when the TO solicitation is limited or restricted to a sole source or brand name in which they are not authorized.

11.4. Award

11.4.1. Accounts

11.4.1.1. Account Requests

Authorized vendors shall submit account requests to the authorized ordering entity in accordance with the authorized ordering entity's review and approval processes.

Authorized vendors shall identify per requested account the required access and permissions.

11.4.1.2. Accounts - Cloud Service Providers

11.4.1.2.1. Existing Accounts

Authorized vendors shall coordinate and support the authorized ordering entities in transferring existing CSP accounts.

11.4.1.2.2. New Accounts

Authorized vendors shall coordinate and support the authorized ordering entities in creating CSP accounts.

11.4.2. Authorized Task Order Services

Authorized vendors shall restrict, by appropriate mean(s) and mechanism(s) (e.g., policy, ACL), authorized ordering entities to only the cloud services (i.e., IaaS, PaaS, SaaS) and / or cloud related IT professional services that have been authorized in accordance with authorized ordering entities awarded TO(s).

11.4.2.1. Exercise of Option Period of Performance

Authorized vendors shall review, update, and validate authorized cloud services and / or cloud related IT professional services on the exercise of an option PoP.

11.4.2.2. Modification(s)

Authorized vendors shall review, update, and validate authorized cloud services and / or cloud related IT professional services on the issuance of TO(s) modifications.

11.4.3. Task Order(s) Kick-Off Meeting

Authorized vendors shall coordinate and schedule within 14 calendar days of TO award notice a TO Kick-Off Meeting **[Deliverable X]** (i.e., physical meeting, virtual meeting).

Authorized vendor's kick-off meeting attendees shall include TO identified key personnel and other appropriate authorized vendor's personnel.

Authorized vendors shall provide a Kick-Off Meeting Agenda in slide format **[Deliverable X]** for review and approval by the authorized ordering entities COR a minimum of 5 calendar days prior to the kick-off meeting. The agenda shall include, at a minimum, the following topics:

- Overview of authorized vendor's POC(s) for all TO task(s) or deliverable(s).
- Overview of authorized vendor's TO organizational structure (e.g., administrative, cybersecurity, management, technical).
- Overview of TO lines of communications between the authorized vendor and the authorized ordering entity (e.g., acquisition, business, cybersecurity, operations, technical).
- Overview of authorized vendor's TO management processes (e.g., costs, performance, risk management, schedule).
- Overview of authorized vendor's transition-in plan.
- Overview of GFI and GFP to be provided to the authorized vendor.
- Overview of authorized vendor's required personnel security clearances and credentials (e.g., HSPD-12).
- Overview of authorized vendor's required personnel access (e.g., facilities, systems), accounts (e.g., user, system), and permissions (e.g., read, write, execute).
- Overview of authorized ordering entity's travel request submissions and approval processes and requirements.
- Overview of authorized ordering entity's purchase request submissions and approval processes and requirements (e.g., OLM purchase requests).
- Overview of TO deliverables (e.g., submission, review, acceptance).
- Overview of TO financial and accounting requirements (e.g., charge codes, CLIN structure).
- Overview of TO risks.

Authorized vendors shall draft and provide a Kick-Off Meeting Minutes Report **[Deliverable X],** within 7 calendar days after the kick-off meeting, documenting the TO kick-off meeting attendees, discussions, decisions, guidance, and action items.

11.5. Post Award

11.5.1. Accounts

11.5.1.1. Account Change Requests

Authorized vendors shall notify authorized ordering entities when account access or permission changes are required (e.g., new accounts, account deletions).

11.5.2. Utilization Based Discounts

Authorized vendors, when using utilization based discounts, shall provide written notification **[Deliverable X]** to authorized ordering entities' ACO at least 60 calendar days prior to the PoP end date that identifies:

- Utilization discounts earned to date for the PoP; and
- Utilization discounts projected to be earned to the PoP end date.

Authorized vendors, when using utilization based discounts, shall provide written notification **[Deliverable X]** to authorized ordering entities ACO within 30 calendar days after the exercise of a PoP (i.e., PoP start date) that identifies:

- Utilization discounts earned and applied to the PoP.

11.5.3. Invoicing

Authorized vendors shall generate and deliver accurate, complete, and timely invoices for cloud services (i.e., IaaS, PaaS, SaaS) and / or cloud-related IT professional services that they are authorized to provide under their awarded TO(s).

11.5.3.1. Authorized Catalog Services

Authorized vendors invoices shall only include the cloud services and / or cloud-related IT professional services that they have provided and been authorized to provide in accordance with their approved service catalogs.

11.5.3.1.1. Unauthorized Catalog Services, Costs

Authorized vendors shall not invoice or otherwise claim costs for unauthorized cloud services and / or cloud-related IT professional services that they have provided and were not authorized to provide in accordance with their approved service catalogs.

11.5.3.2. Authorized Task Order(s) Services

Authorized vendors invoices shall only include the cloud services and / or cloud-related IT professional services that they have provided and been authorized to provide in accordance with their awarded TO(s).

11.5.3.2.1. Unauthorized Task Order(s) Services, Costs

Authorized vendors shall not invoice or otherwise claim costs for unauthorized cloud services and / or cloud-related IT professional services that they have provided and were not authorized to provide in accordance with their awarded TO(s).

11.5.3.3. Erroneous Calculations, Configurations, Settings

Authorized vendors shall not invoice or otherwise claim costs for cloud services and / or cloud-related IT professional services that resulted from authorized vendors' erroneous calculations, configurations, or settings.

11.5.3.4. Invoicing Fixed Price (FP), Labor Hour (LH)

11.5.3.4.1. Data Elements

Authorized vendors FP and LH invoice(s) shall include the required data elements and may include the optional data elements. (Reference Appendix F)

Data elements that have no value or are NA shall have a value of "NULL".

1827

Table 13: Invoicing FP, LH Required Data Elements			
Data Element	Format	Examples / **[Valid Values]**	Notes
BPA Award Number	Alphanumeric	01ABC123	
TO Award Number	Alphanumeric	02DEF456	
TO PoP	Numerical	00, 01, 02, 03	
TO PoP Start Date	YYYY MM DD	2022 01 01	
TO PoP End Date	YYYY MM DD	2022 12 31	
TO CLIN	Numerical, Alphanumeric	1001, 0001A, A001	
To Sub-CLIN	Numerical, Alphanumeric	1001, 0001A, A001	
TO CLIN Type	Text	**[FFP, FP, FUP, LH]**	
Service Name	Text	Large Server, Cybersecurity Forensics	

CSP Identifier / Cloud Related IT Professional Service Code	Text, Numerical, Alphanumeric	ABCDEFGHI, 1234567890, A1B2C3D4E5F6	1. Identifies the CSP's unique code (e.g., UPC) for each cloud service and is universal across resellers. The "CSP Identifier" should also be universal across commercial and non-commercial (e.g., government) customers. 2. Shall match the "CSP Identifier" from the authorized vendor's BPA catalog for the service. 3. The authorized vendor shall receive the "Cloud Related IT Professional Service Code(s)" from the administrative agency.
Service Start Date	YYYY MM DD	2022 07 01	Identifies the date that the service began incurring costs (e.g., billable start date) within the invoice period.
Service End Date	YYYY MM DD	2022 07 31	Identifies the date that the service stopped incurring costs (e.g., billable start date) within the invoice period.
Catalog Service Price	Currency	$5.4321	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the service price for a quantity of one (1), from the authorized vendor's BPA catalog, for the service in US currency (i.e., US dollars) out to four (4) decimal places (i.e., ten-thousandths) for cloud services and out to two (2) decimal places (i.e., hundredths) for cloud-related IT professional services.
Service Price Discount	Percentage	8.5%, 12%	If the TO negotiated a percentage(s) discount from the authorized vendor's catalog, or subset of services from the catalog, the percentage discount shall be listed. If the TO negotiated individual and discrete prices per service, the "Service Price Discount" shall have a value of "NULL".

TO Service Price	Currency	$5.4321	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the TO service price in US currency (i.e., US dollars) out to four (4) decimal places (i.e., ten-thousandths) for cloud services and out to two (2) decimal places (i.e., hundredths) for cloud-related IT professional services.
Unit of Measure	Text	Labor Hour, Compute per Hour, Subscription	
Quantity	Numerical	1, 1.5, 25, 1,234	
Total Cost	Currency	$56.98	1. Identifies the total price in US currency (i.e., US dollars) out to four (4) decimal places (i.e., ten-thousandths) for cloud services and out to two (2) decimal places (i.e., hundredths) for cloud-related IT professional services. 2. "Total Cost" = "TO Service Price" x "Quantity"

1828

Table 14: Invoicing FP, LH Optional Data Elements

Data Element	Format	Examples / **[Valid Values]**	Notes
SKU	Text, Numerical, Alphanumeric	ABCDEFGHI, 1234567890, A1B2C3D4E5F6	

1829

11.5.3.5. Invoicing Time and Materials

11.5.3.5.1. Data Elements

Authorized vendors T&M invoice(s) shall include the required data elements and may include the optional data elements. (Reference Appendix G)

Data elements that have no value or are NA shall have a value of "NULL".

Table 15: Invoicing T&M Required Data Elements

Data Element	Format	Examples / **[Valid Values]**	Notes
BPA Award Number	Alphanumeric	01ABC123	
TO Award Number	Alphanumeric	02DEF456	
TO PoP	Numerical	00, 01, 02, 03	
TO PoP Start Date	YYYY MM DD	2022 01 01	
TO PoP End Date	YYYY MM DD	2022 12 31	
TO CLIN	Numerical, Alphanumeric	1001, 0001A, A001	
To Sub-CLIN	Numerical, Alphanumeric	1001, 0001A, A001	

TO CLIN Type	Text	T&M	
Service Name	Text	Large Server, Cybersecurity Forensics	
CSP Identifier / Cloud Related IT Professional Service Code	Text, Numerical, Alphanumeric	ABCDEFGHI, 1234567890, A1B2C3D4E5F6	1. Identifies the CSP's unique code (e.g., UPC) for each cloud service and is universal across resellers. The "CSP Identifier" should also be universal across commercial and non-commercial (e.g., government) customers. 2. Shall match the "CSP Identifier" from the authorized vendor's BPA catalog for the service. 3. The authorized vendor shall receive the "Cloud Related IT Professional Service Code(s)" from the administrative agency.
Service Start Date	YYYY MM DD	2022 07 01	Identifies the date that the service began incurring costs (e.g., billable start date) within the invoice period.
Service End Date	YYYY MM DD	2022 07 31	Identifies the date that the service stopped incurring costs (e.g., billable start date) within the invoice period.
Catalog Service Price:	Currency	$5.4321	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the service price for a quantity of one (1), from the authorized vendor's BPA catalog, for the service in US currency (i.e., US dollars) out to four (4) decimal places (i.e., ten-thousandths) for cloud services and out to two (2) decimal places (i.e., hundredths) for cloud-related IT professional services.
TO Ceiling Price	Currency	$5.4321	1. All currency values are to be denominated in US currency (i.e., US dollars).

			2. Identifies the service maximum allowable price for quantity of one (1), allowable under the awarded TO, for the service in US currency (i.e., US dollars) out to four (4) decimal places (i.e., ten-thousandths) for cloud services and out to two (2) decimal places (i.e., hundredths) for cloud-related IT professional services.
Direct Costs	Currency	$6.75	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the summation of all allowable direct costs (e.g., direct labor, fringe benefits) for the service in US currency (i.e., US dollars) out to two (2) decimal places (i.e., hundredths).
Indirect Costs	Currency	$9.34	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the summation of all allowable indirect costs (e.g., overhead, G&A) for the service in US currency (i.e., US dollars) out to two (2) decimal places (i.e., hundredths).
Fixed Handling Factor	Currency	$2.45	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the TO negotiated fixed handling factor for the service in US currency (i.e., US dollars) out to two (2) decimal places (i.e., hundredths).
Profit	Currency	$4.15	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the TO negotiated profit for the service in US currency (i.e., US dollars) out to two (2) decimal places (i.e., hundredths).

Unit of Measure	Text	Labor Hour, Flight	
Quantity	Numerical	1, 1.5, 25, 1,234	
Total Cost	Currency	$56.98	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. "Total Cost" = ("Direct Costs" + "Indirect Costs" + "Fixed Handling Factor" + "Profit") x "Quantity"

:

Table 16: Invoicing T&M Optional Data Elements

Data Element	Format	Examples / **[Valid Values]**	Notes
SKU	Text, Numerical, Alphanumeric	ABCDEFGHI, 1234567890, A1B2C3D4E5F6	

1837

11.5.3.6. Invoicing Format

Authorized vendors shall provide invoices in the required format. (Sample References: Appendix F & G)

11.5.3.7. Invoicing Submissions

Authorized vendors shall submit invoices to the authorized ordering entities no less than once per month (i.e., monthly) for the cloud services and / or the cloud-related IT professional services provided.

Authorized vendors shall include, with invoice submissions to the authorized ordering entities, the automated invoice validation confirmation.

11.5.3.8. Invoicing Validation

Authorized vendors shall submit all invoices to the BPA Contracting Officer's automated invoice validation service prior to invoice submissions to the authorized ordering entity.

Authorized vendors shall review and resolve all identified disconnects, inconsistencies, errors, and other anomalies identified by the automated validation service prior to invoice submissions to the authorized ordering entity.

11.5.3.9. Paid Invoices

Authorized vendors shall provide the BPA Administering Agency, at least monthly, with copies of all authorized ordering entities paid invoices **[Deliverable X]**

11.5.4. Past Performance Evaluations

Authorized vendors shall submit comments, rebutting statements, or additional information within 14 calendar days of CPARS system notifications of availability of past performance evaluations.

11.5.5. Networking and Routing

Authorized vendors shall coordinate with and provide authorized ordering entities with required networking (e.g., MAC addresses) and routing configuration information (e.g., IP addresses) to allow authorized ordering entities to configure authorized ordering entities' networks (e.g., firewalls, MTIPS, TIC) to connect to authorized vendors' cloud services (i.e., IaaS, PaaS, SaaS).

11.5.6. Non-Personal Services

Authorized vendors shall immediately notify the ACO and COR, for the respective awarded TO, if an authorized vendor believes that any actions constitute or are perceived to constitute personal services.

11.5.7. Points of Contact

Authorized vendors shall identify per awarded TO(s) the authorized vendor's POC responsible for addressing and responding to communications, concerns, inquiries, or issues from the authorized ordering entities for the following minimum areas of responsibilities.

Table 17: Authorized Vendor's Point of Contacts

Position	Name	Title	Email Address
Acquisitions			
Cybersecurity			
Financial / Invoicing			
Program / Project Management			
Purchase Requests			
Technical			
Travel			

Authorized vendors may identify one (1) or more of the same or different POCs for each area of responsibility.

11.5.8. Services Summary Report

Authorized vendors shall deliver to authorized ordering entities a Services Summary Report **[Deliverable X]** at the end of each FFP PoP. The Services Summary Report shall be delivered within 30 days after the end of each FFP PoP.

The Services Summary Report shall not include detailed cost information.

11.5.8.1. Required Data Elements

The Services Summary Report (Reference Appendix H) shall include the following minimum required data elements as follows:

Data elements that have no value or are NA shall have a value of "NULL".

1892

Table 18: Service Summary Report			
Data Element	Format	Examples or **[Valid Values]**	Notes
BPA Award Number	Alphanumeric	01ABC123	
TO Award Number	Alphanumeric	02DEF456	
TO PoP	Numerical	00, 01, 02, 03	
TO PoP Start Date	YYYY MM DD	2022 01 01	
TO PoP End Date	YYYY MM DD	2022 12 31	
TO CLIN	Numerical, Alphanumeric	1001, 0001A, A001	
Service Name	Text	Large Server, Cybersecurity Forensics	
CSP Identifier / Cloud Related IT Professional Service Code	Text, Numerical, Alphanumeric	ABCDEFGHI, 1234567890, A1B2C3D4E5F6	1. Identifies the CSP's unique code (e.g., UPC) for each cloud service and is universal across resellers. The "CSP Identifier" should also be universal across commercial and non-commercial (e.g., government) customers. 2. Shall match the "CSP Identifier" from the authorized vendor's BPA catalog for the service. 3. The authorized vendor shall receive the "Cloud Related IT Professional Service Code(s)" from the BPA Contracting

			Officer.
Average Service Utilization Rate	Percentage	75%, 98%, NULL	Identifies the average utilization of the cloud service (i.e., IaaS, PaaS, SaaS) during the PoP.
Unit of Measure	Text	Labor Hour, Compute per Hour, Subscription, NULL	
Cost Element		**[Cost, No Cost]**	Identifies if the cloud service (i.e., IaaS, PaaS, SaaS) incurred a cost or no cost to the authorized vendor.

1893

11.5.9. Expanded Transactional Data Reporting

RESERVED - TBD

11.5.10. Travel

11.5.10.1. Task Order(s) Travel Requests

Authorized vendors shall submit their travel requests to authorized ordering entities in accordance with the authorized ordering entities requirements (e.g., timeframe, format, information).

11.5.10.2. Task Order(s) Travel Documentation

Authorized vendors shall be responsible for obtaining all necessary travel documents (e.g., passports, Visas, medical tests) required to execute travel.

11.5.10.3. Task Order(s) Travel Invoices

Authorized vendors shall invoice for incurred travel costs within 60 calendar days of the completion of each approved travel.

Authorized vendors shall include all required supporting documentation (e.g., receipts) for each approved travel with the travel invoices.

12. Pool 1: Infrastructure as a Service, Platform as a Service

Authorized vendors shall provide IaaS and PaaS solutions in accordance with the following requirements.

12.1. Acquisition Requirements

RESERVED

12.1.1. Authorized Task Order(s) Services

Authorized vendors shall provide a mean(s) and mechanism(s) (e.g., policy, ACL) to restrict authorized ordering entities to only the IaaS and PaaS cloud

services that have been authorized in accordance with the authorized ordering entities' awarded TO(s).

12.1.2. Section 508 Compliance

Authorized vendors shall provide Iaas and Paas cloud services that are compliant with Section 508 of the *Rehabilitation Act (29 U.S.C. 794d)* and Section 255 of the *Telecommunications Act of 1996 (47 U.S.C. 255)*.[103, 104]

Authorized vendors shall provide the BPA Contracting Officer with a VPAT(™) for each IaaS and PaaS CSO.[105]

Authorized vendors shall ensure the VPAT(™) on file with the BPA Contracting Officer remains accurate and up to date for each IaaS and PaaS CSO.

12.1.2.1. Task Order(s), Section 508 Compliance

Authorized ordering entities are authorized to identify additional Section 508 Compliance requirements at the TO level.

12.1.2.2. Task Order(s), Section 508 Exceptions

Authorized ordering entities shall identify Section 508 exceptions at the TO level.

12.2. Business Requirements

RESERVED

12.2.1. Costs Management

Authorized vendors shall provide an interactive Graphical User Interface (GUI) (e.g., dashboard, portal) that allows authorized ordering entities to manage and monitor IaaS and PaaS cloud services costs (i.e., measured services).

12.2.1.1. Budgets

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to enter and establish budgets for each IaaS and PaaS cloud service.

[103] FAR 39.2 Information and Communication Technology
[104] 36 CFR 1194 Information and Communications Technology Standards and Guidelines
[105] Executive Order 14035: Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce

12.2.1.2. Budget Notifications

Authorized vendors shall provide a mean(s) and mechanism(s) (e.g., email, SMS) that notifies authorized ordering entities when an IaaS or PaaS cloud service has incurred costs exceeding the defined thresholds of 50%, 75%, and 100% of their budgets.

12.2.1.3. Cost Allocation Tag(s)

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to establish and assign cost allocation tag(s) (e.g., application, environment, office, program) for each IaaS and PaaS cloud service.

The default cost allocation tag shall be the authorized ordering entity.

12.2.1.4. Cost Information

12.2.1.4.1. Application Programming Interfaces (APIs), Cost Information

Authorized vendors shall provide secure API(s) and / or Electronic Data Interchange (EDI)(s) that allows authorized ordering entities to access and download (i.e., pull) directly, and by third party applications, their:

- Real-time cost information, required data elements
- Archived cost information, required data elements datasets.

The downloaded datasets shall be identical (e.g., completeness, granularity, periodicity) to the datasets used for the respective required interactive GUIs.

The downloaded data sets shall not be more than 15 minutes older (objective) than the datasets used for the respective required interactive GUIs.

Authorized ordering entities, by the provided secure API(s) and / or EDI(s), shall be able to identify the datasets date range (e.g., Jan 1, 2021 to Jan 21, 2021) and duration (e.g., 7 days, 45 days, 115 days), within the active and expired PoP(s) (e.g., sliding window), for download.

12.2.1.4.2. Real-Time Cost Information

Authorized vendors shall provide an interactive GUI (e.g., dashboard, portal) that displays and presents, for the active and PoP, the following required real-time cost data elements, updated at a minimum within the past 24 hours, for each IaaS and PaaS cloud service used by an authorized ordering entity (i.e., measured service).

1978

Table 19: Real-Time Cost Information Required Data Elements			
Data Element	Format	Examples / **[Valid Values]**	Notes
Service Name	Text	Large Server	
Operational Status	Text	Active, Suspended, Terminated	
Budgeted Costs	Currency	$15,000.00	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the budgeted value entered by the authorized vendors or authorized ordering entities. If no "Budgeted Costs" has been established a value of "Null" shall be displayed.
Costs to Date	Currency	$6,500.50	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the total cumulative cost to date for the cloud service during the active PoP (e.g., currently executing PoP).
Costs Projection, 7 Days	Currency	$7,500.75	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the estimated "Costs to Date" plus (+) seven (7) days into the future.
Costs Projection, 30 Days	Currency	$10,100,10	1. All currency values are to be denominated in US currency (i.e., US dollars).

			2. Identifies the estimated "Costs to Date" plus (+) thirty (30) days into the future.
Costs Expenditure, 50%	YYYY MM DD	2021 03 15	Identifies the estimated date in which 50% of the "Budgeted Costs" will be expended or the date on which 50% of the "Budgeted Costs" were expended.
Costs Expenditure, 75%	YYYY MM DD	2021 06 15	Identifies the estimated date in which 75% of the "Budgeted Costs" will be expended or the date on which 75% of the "Budgeted Costs" were expended.
Costs Expenditure, 100%	YYYY MM DD	2021 09 30	Identifies the estimated date in which 100% of the "Budgeted Costs" will be expended or the date on which 100% of the "Budgeted Costs" were expended.
Cost Allocation Tag(s)	Text	Payroll, Development, Human Resources	1. Identifies the cost allocation value(s) entered by the authorized ordering entity. 2. The default "Cost Allocation Tag" shall be the authorized ordering entity.

Authorized ordering entities shall be able to isolate and view cost information for any date range (e.g., Jan 1, 2021 to Jan 21, 2021) and duration (e.g., 7 days, 45 days, 115 days) within the active PoP (e.g., sliding window).

2.2.1.4.3. Archived Cost Information

Authorized vendors shall provide an interactive GUI (e.g., dashboard, portal) that displays and presents, for expired PoP(s), the following required archived cost data elements for each IaaS and PaaS cloud services used by an authorized ordering entity (i.e., measured services).

Table 20: Archived Cost Information Required Data Elements

Data Element	Format	Examples / **[Valid Values]**	Notes
Service Name	Text	Large Server	
Budgeted Costs	Currency	$15,000.00	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the budgeted value entered by the authorized vendors or authorized ordering entities. If no "Budgeted Costs" has been established a value of "Null" shall be displayed.
Costs to Date	Currency	$14,950.00	1. All currency values are to be denominated in US currency (i.e., US dollars). 2. Identifies the total cumulative cost for the cloud service during the expired PoP(s).
Cost Allocation Tag(s)	Text	Payroll, Development, Human Resources	1. Identifies the cost allocation value(s) entered by the authorized ordering entity. 2. The default "Cost Allocation Tag" shall be the authorized ordering entity.

1986

12.3. Cybersecurity Requirements

12.3.1. Cybersecurity Notifications and Acknowledgements

Authorized vendors shall provide a mean(s) and mechanism(s) that notifies at a minimum the authorized ordering entities cybersecurity POC(s) of cybersecurity announcements, bulletins, watches, warnings, etc.

Authorized vendors shall provide a mean(s) and mechanism(s) that requires the authorized ordering entities cybersecurity POC(s) to acknowledge the cybersecurity announcements, bulletins, warnings, etc.

Authorized vendors shall provide a mean(s) and mechanism(s) that records the authorized ordering entities cybersecurity POC(s) acknowledgement of the cybersecurity announcements, bulletins, watches, warnings, etc.

12.3.1.1. Application Programming Interfaces, Cybersecurity Notifications

Authorized vendors shall provide secure API(s) and / or EDI(s) that allows authorized vendors to push and download to authorized ordering entities and third-party applications:

- Cybersecurity notifications.

The pushed and downloaded notifications information shall be identical to the notifications information that authorized ordering entities cybersecurity POC(s) receive.

The pushed and downloaded notifications information shall not be more than 15 minutes older (objective) than the notifications information that authorized ordering entities cybersecurity POC(s) receive.

Authorized ordering entities, by the provided secure API(s) and / or EDI(s), shall be able to identify the notification date range (e.g., Jan 1, 2021 to Jan 21, 2021) and duration (e.g., 7 days, 45 days, 115 days), within the active and expired PoP(s) (e.g., sliding window), for download.

12.3.2. Cybersecurity Tag(s)

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to establish and assign cybersecurity tag(s) to each IaaS and PaaS cloud services (e.g., compliance, FIPS, access control).

12.3.3. Identity and Access Management

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to perform identity management and access management (i.e., IAM) for each IaaS and PaaS cloud service.

12.3.3.1. Application Programming Interfaces, Identity and Access Management

Authorized vendors shall provide secure API(s) and / or EDI(s) that allows authorized ordering entities, directly and by third party applications, to perform identity management and access management (i.e., IAM) for each IaaS and PaaS cloud service.

Authorized ordering entities, by the provided secure API(s) and / or EDI(s), shall be able to configure identities (i.e., add, modify, delete) and permissions (i.e., read, write, execute) for each IaaS and PaaS cloud service.

12.3.3.2. Identity Management

Authorized vendors' identity management shall support at a minimum the addition, modification, and deletion of digital (e.g., application, hardware) and user (e.g., individual, role, group) identities.

User identities at a minimum shall include individual, role, and group identities.

12.3.3.3. Access Management

Authorized vendors' access management shall allow authorized ordering entities to configure and assign access permissions on a digital (e.g., application) and individual (e.g., John Smith), role (e.g., admin, cloud engineer), and group (e.g., cybersecurity team, financial team) basis.[106]

Access permissions at a minimum shall include read, write, and execute.

12.4. Environmental Requirements[107]

12.4.1. Carbon Pollution-Free Electricity (CFE)

Authorized vendors shall power (i.e., electrify) their data centers, providing IaaS and PaaS cloud services, using carbon pollution-free electricity (e.g., geothermal, hydroelectric, hydrokinetic, nuclear, solar, wind).

[106] NIST, SP 800-210: General Access Control Guidance for Cloud Systems
[107] GSAM 552.238-78 Identification of Products that Have Environmental Attributes

Authorized vendors shall achieve the following carbon pollution-free electricity minimum percentage rates by the following dates.

Table 21: Carbon Pollution-Free Electricity	
Minimum Percentage	Date
<<X%>	<<December 31, 20XX>>
75%	December 31, 2028
100%	December 31, 2030

12.4.1.1. Exclusion, Emergency and Standby Power

Data center power (i.e., electricity) from emergency and standby power backup systems (e.g., fossil fuel generators, gas turbines) are excluded from the CFE minimum percentage calculation.

12.4.1.2. Exclusion, Declared Disasters and Emergencies

Data center power (i.e., electricity) from non-CFE sources are excluded from the CFE minimum percentage calculation when CFE sources are negatively impacted (e.g., cost, generation, reliability, sine waveform (e.g., amplitude, frequency, phase), stability, transmission) by declared disasters or emergencies that may be natural or man-made, including acts of terrorism (e.g., biological, chemical, nuclear, radiological). Disasters or emergencies may be declared by local, state, tribal, or federal authorities to include NERC (i.e., ERO for the US) and Regional Entities (i.e., MRO, NPCC, RF, SERC, Texas RE, WECC).

12.4.2. Energy Efficiency

Authorized vendors shall provide IaaS and PaaS cloud services that use ENERGY STAR® or EPEAT certified hardware.

12.4.2.1. Task Order(s), Energy Efficiency

Authorized ordering entities are authorized to identify additional energy efficiency requirements at the TO level.

12.5. Operational Requirements

12.5.1. Operational Management

Authorized vendors shall provide an interactive GUI (e.g., dashboard, portal) that allows authorized ordering entities to activate, configure, suspend, and terminate each IaaS and PaaS cloud services (i.e., on-demand self-service).

12.5.1.1. Application Programming Interfaces, Operational Management

Authorized vendors shall provide secure API(s) and / or EDI(s) that allows authorized ordering entities, directly and by third party applications, to activate, configure, suspend, and terminate each IaaS and PaaS cloud services (i.e., on-demand self-service).

Authorized ordering entities, by the provided secure API(s) and / or EDI(s), shall be able to configure:

- Autoscaling (e.g., autoscaling thresholds) for each IaaS and PaaS cloud services.

12.5.1.2. Automation

12.5.1.2.1. Task Order(s), Automation

Authorized ordering entities are authorized to identify additional automation requirements at the TO level.

12.5.1.3. Autoscaling

Authorized vendors shall provide a mean(s) and mechanism(s) that allows each IaaS and PaaS cloud services to autoscale up and down based on utilization (e.g., demand).

12.5.1.3.1. Autoscaling Thresholds

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to establish autoscaling utilization thresholds (e.g., triggers, scale up at 90% utilization, scale down at 25% utilization) for each IaaS and PaaS cloud service.

12.5.1.3.2. Autoscaling Minimum

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to establish a minimum (e.g., floor, 1 compute instance) for each IaaS and PaaS cloud service.

12.5.1.3.3. Autoscaling Maximum

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to establish a maximum (e.g., ceiling, 5 compute instances) for each IaaS and PaaS cloud service.

12.5.1.4. Automation Tag(s)

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to establish and assign automation tag(s) to each IaaS and PaaS cloud services (e.g., autoscaling, operating hours, rapid elasticity).

12.5.1.5. Technical Tag(s)

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities to establish and assign technical tag(s) to each IaaS and PaaS cloud service (e.g., domain, environment, license, location, OS).

12.5.1.6. Operational Information

12.5.1.6.1. Application Programming Interfaces, Operational Information

Authorized vendors shall provide secure API(s) and / or EDI(s) that allows authorized ordering entities to access and download (i.e., pull) directly, and by third party applications, their:

- Real-time operational information, required data elements;
- Historical operational information, required data elements; and
- Archived operational information, required data elements datasets.

The downloaded data sets shall be identical (e.g., completeness, granularity, periodicity) to the datasets used for the respective required interactive GUIs.

The downloaded datasets shall not be more than 15 minutes older (objective) than the datasets used for the respective required interactive GUIs.

Authorized ordering entities, by the provided secure API(s) and / or EDI(s), shall be able to identify the datasets date range (e.g., Jan 1, 2021 to Jan 21, 2021) and duration (e.g., 7 days, 45 days, 115 days), within the active and expired PoP(s) (e.g., sliding window), for download.

12.5.1.6.2. Real-Time Operational Information

Authorized vendors shall provide an interactive GUI (e.g., dashboard, portal) that displays and presents the following required real-time operational information, for the past 24 hours, for each IaaS and PaaS cloud services used by an authorized ordering entity (i.e., measured services).

2139

Table 22: Real-Time Operational Information Required Data Elements			
Data Element	Format	Examples / **[Valid Values]**	Notes
Service Name	Text	Large Server	
Operational Status	Text	Active, Suspended, Terminated	
Performance Status	Text	Operational, Degraded, Interrupted, Down	Identifies the current performance status of the cloud service reported by the CSP.
Operational Notifications	Text, URL	Notice of Maintenance, www.maintenance.com	Identifies if the cloud service has a planned future operational activity (e.g., emergency maintenance, maintenance window, service discontinuation) and either displays the information directly or provides a URL to information resources.
Uptime	Days:Hours: Minutes: Seconds	364:23:45:59	Identifies the total cumulative time (e.g., duration) that the cloud service has been active during the PoP (e.g., currently executing PoP). Only cloud services that are in an active status accumulate uptime.
Utilization Rate - Average	Percentage	85%	
Utilization Rate - Mean	Percentage	80%	
Utilization Rate - Peak	Percentage	99%	
Utilization Rate - Minimum	Percentage	55%	
Energy Efficient Cloud	Text, Image	Yes, No, EPEAT(™)	Identifies if the cloud service operates on EPEAT(™) or

Service[108]		Logo, ENERGY STAR® Logo	ENERGY STAR® Certified equipment (e.g., servers, storage, networking equipment).
Service Allocation Tag(s)	Text	Email, Payroll, Website	1. Identifies the service allocation value(s) entered by the authorized ordering entity. 2. The default "Service Allocation Tag" shall be the authorized ordering entity.
Automation Tag(s)	Text	Weekdays Only, Decommission Date	
Cybersecurity Tag(s)	Text	HIPPA, Government Only, DB Team	
Technical Tag(s)	Text	gsa.gov, Test, CSP Data Center, Linux	

Authorized ordering entities shall be able to isolate and view real-time operational information for any time period (e.g., 12:30 PM to 1:45 PM) within the previous 24 hours (e.g., sliding window).

[108] GSAM 552.238-78 Identification of Products that Have Environmental Attributes

2143

2144 **12.5.1.6.3. Historical Operational Information**

2145 Authorized vendors shall provide an interactive GUI (e.g., dashboard, portal) that displays and presents, for the active
2146 PoP, the following required historical operational information for each IaaS and PaaS cloud services used by an
2147 authorized ordering entity (i.e., measured services).

Table 23: Historical Operational Information Required Data Elements

Data Element	Format	Examples / **[Valid Values]**	Notes
Service Name	Text	Large Server	
Operational Status	Text	Active, Suspended, Terminated	
Uptime	Days:Hours: Minutes: Seconds	364:23:45:59	Identifies the total cumulative time (e.g., duration) that the cloud service has been active during the PoP (e.g., currently executing PoP). Only cloud services that are in an active status accumulate uptime.
Utilization Rate - Average	Percentage	90%	
Utilization Rate - Mean	Percentage	87%	
Utilization Rate - Peak	Percentage	99%	
Utilization Rate - Minimum	Percentage	55%	
Energy Efficient Cloud	Text, Image	Yes, No, EPEAT(™) Logo, ENERGY STAR®	Identifies if the cloud service operates on EPEAT (™) or ENERGY STAR® Certified equipment (e.g., servers, storage,

Service[109]		Logo	networking equipment).
Service Allocation Tag(s)	Text	Email, Payroll, Website	1. Identifies the service allocation value(s) entered by the authorized ordering entity. 2. The default "Service Allocation Tag" shall be the authorized ordering entity.
Automation Tag(s)	Text	Weekdays Only, Decommission Date	
Cybersecurity Tag(s)	Text	HIPPA, Government Only, DB Team	
Technical Tag(s)	Text	gsa.gov, Test, CSP Data Center, Linux	

Authorized ordering entities shall be able to isolate and view historical operational information for any date range (e.g., Jan 1, 2021 to Jan 21, 2021) and duration (e.g., 7 days, 45 days, 115 days) within the active PoP (e.g., sliding window).

[109] GSAM 552.238-78 Identification of Products that Have Environmental Attributes

12.5.1.6.4. Archived Operational Information

Authorized vendors shall provide an interactive GUI (e.g., dashboard, portal) that displays and presents, for expired PoP(s), the following required archived operational information for each IaaS and PaaS cloud services used by an authorized ordering entity (i.e., measured services).

Table 24: Archived Operational Information Required Data Elements

Data Element	Format	Examples / **[Valid Values]**	Notes
Service Name	Text	Large Server	
Uptime	Days:Hours: Minutes: Seconds	364:23:45:59	Identifies the total cumulative time (e.g., duration) that the cloud service has been active during the PoP (e.g., currently executing PoP). Only cloud services that are in an active status accumulate uptime.
Utilization Rate - Average	Percentage	90%	
Utilization Rate - Mean	Percentage	87%	
Utilization Rate - Peak	Percentage	99%	
Utilization Rate - Minimum	Percentage	55%	
Energy Efficient Cloud Service[110]	Text, Image	Yes, No, EPEAT(™) Logo, ENERGY STAR® Logo	Identifies if the cloud service operates on EPEAT (™) or ENERGY STAR® Certified equipment (e.g., servers, storage, networking equipment).
Service Allocation Tag(s)	Text	Email, Payroll, Website	1. Identifies the service allocation value(s) entered by the

[110] GSAM 552.238-78 Identification of Products that Have Environmental Attributes

			authorized ordering entity. 2. The default "Service Allocation Tag" shall be the authorized ordering entity.
Automation Tag(s)	Text	Weekdays Only, Decommission Date	
Cybersecurity Tag(s)	Text	HIPPA, Government Only, DB Team	
Technical Tag(s)	Text	gsa.gov, Test, CSP Data Center, Linux	

2159

12.5.2. Operational Notifications

Authorized vendors shall provide a mean(s) and mechanism(s) that allows authorized ordering entities (e.g., IT employees) to subscribe and receive (e.g., email, telephone call, SMS) cloud services operational notifications.

12.5.2.1. Application Programming Interfaces, Operational Notifications

Authorized vendors shall provide secure API(s) and / or EDI(s) that allows authorized vendors to push and download to authorized ordering entities and third-party applications:

- Emergency Maintenance Windows
- Negative Service Performance
- Planned Maintenance Windows
- Service Discontinuations notifications

The pushed and downloaded notifications information shall be identical to the notifications information that authorized ordering entities are able to subscribe to and receive (e.g., email, telephone call, SMS).

The pushed and downloaded notifications information shall not be more than (15 minutes) older (objective) than the notifications information that authorized ordering entities are able to subscribe to and receive.

Authorized ordering entities, by the provided secure API(s) and / or EDI(s), shall be able to identify the notification date range (e.g., Jan 1, 2021 to Jan 21, 2021) and duration (e.g., 7 days, 45 days, 115 days), within the active and expired PoP(s) (e.g., sliding window), for download.

12.5.2.2. Notification of Emergency Maintenance Windows

Authorized vendors shall notify authorized ordering entities of emergency maintenance windows as soon as possible.

Emergency maintenance window notifications will identify the following:

- Date and Time of Emergency Maintenance Window;
- Estimated Duration of Emergency Maintenance Window;
- Cloud Services Impacted;
- Emergency Maintenance Window Information or URL to Information Resource(s); and
- Emergency Maintenance Window POC(s).

Authorized vendors shall notify authorized ordering entities when the emergency maintenance window has concluded. The notification shall identify if authorized ordering entities are required to perform any actions (e.g., restart, reconfigure).

12.5.2.3. Notification of Negative Service Performance

Authorized vendors shall notify authorized ordering entities of negative or degraded cloud service(s) performance as soon as possible.

Negative service performance notifications will identify the following:

- Nature of Negative Service Performance (e.g., Degraded, Interrupted, Down);
- Estimated Duration of Negative Service Performance;
- Cloud Services Impacted;
- Negative Service Performance Information or URL to Information Resource(s); and
- Negative Service Performance POC(s).

Authorized vendors shall notify authorized ordering entities when the negative service performance has been resolved. The notification shall identify if authorized ordering entities are required to perform any actions (e.g., restart, reconfigure).

12.5.2.4. Notification of Planned Maintenance Windows

Authorized vendors shall notify authorized ordering entities of planned maintenance windows a minimum of 30 days, 7 days, and 24 hours in advance.

Planned maintenance window notifications will identify the following:

- Date and Time of Planned Maintenance Window;
- Duration of Planned Maintenance Window;
- Cloud Service(s) Impacted;
- Planned Maintenance Window Information or URL to Information Resource(s); and
- Planned Maintenance Window POC(s).

Authorized vendors shall notify authorized ordering entities when the planned maintenance window has concluded. The notification shall identify if authorized ordering entities are required to perform any actions (e.g., restart, reconfigure).

12.5.2.5. Notification of Service Discontinuations

Authorized vendors shall notify authorized ordering entities of planned cloud service(s) discontinuations (e.g., sunsetting, termination) a minimum of 180 days, 90 days, 60 days, 30 days, 7 days, and 24 hours in advance.

Service discontinuation notifications will identify the following:

- Date and Time of Service(s) Discontinuation;
- Cloud Service(s) to be Discontinued;
- Service(s) Discontinuation Information or URL to Information Resource(s); and
- Service(s) Discontinuation POC(s).

12.5.3. Operational Support

Authorized vendors shall provide 24x7x365 operational support to authorized ordering entities.

12.5.3.1. Tier 0 Operational Support

Authorized vendors shall provide Tier 0 operational support, to authorized ordering entities, that consists of self-help and user-retrieved information support (e.g., blog posts, community forums, FAQ, how-tos, manuals, technical information, training).

12.5.3.2. Tier 1 Operational Support

Authorized vendors shall provide Tier 1 operational support, to authorized ordering entities, that is responsible for capturing all pertinent information required to resolve requests, incidents, and work orders and appropriately triaging and prioritizing tickets.

Tier 1 operational support consists of resources responsible for resolving basic and standard requests, incidents, and work order for the authorized vendor's IaaS and PaaS cloud services.

12.5.3.3. Tier 2 Operational Support

Authorized vendors shall provide Tier 2 operational support, to authorized ordering entities, that is responsible for resolving requests, incidents, and work orders that cannot be processed or resolved by the Tier 1.

Tier 2 operational support consists of resources that are experienced and knowledgeable in troubleshooting the authorized vendor's IaaS and PaaS cloud services.

12.5.3.4. Tier 3 Operational Support

Authorized vendors shall provide Tier 3 operational support, to authorized ordering entities, that is responsible for resolving requests, incidents, and work orders that cannot be processed or resolved by either Tier 1 or Tier 2.

Tier 3 operational support consists of the highest level of resources that have specialized experience and knowledge in troubleshooting the authorized vendor's IaaS and PaaS cloud services.

12.5.3.5. Task Order(s) Operational Support

Authorized ordering entities are authorized to identify additional operational support requirements at the TO level.

12.6. Technical Requirements

12.6.1. Data Centers, High Availability

Authorized vendors shall provide IaaS and PaaS cloud services from a minimum of two HA data centers.

Under this section a HA data center shall be defined as a data center that has been designed for and operates at a minimum of 99.99% availability (i.e., four 9s).

12.6.1.1. Connectivity Connections

Authorized vendors shall provide HA data centers with at least two separate connectivity connections.

12.6.1.2. Bandwidth

Authorized vendors shall provide connectivity connections with a minimum bandwidth of 100 Gbps per connection.

12.6.1.3. Geographically Diverse

Authorized vendors shall provide data centers that are geographically diverse to ensure natural events or disasters (e.g., earthquakes, floods, forest fires,

hurricanes) do not impact the operations of the data centers simultaneously (e.g., at the same time).

12.6.1.3.1. High Risk Flood Areas

Authorized vendors shall provide HA data centers that are not located in high-risk flood geographical areas as identified by DHS FEMA National Flood Hazard Layer (NFHL).

12.6.1.3.2. North American Electric Reliability Corporation Interconnections

Authorized vendors shall provide HA data centers that are not located within the same North American Electric Reliability Corporation (NERC) interconnections (i.e., Alaska Interconnection, Eastern Interconnection, Texas Interconnection, Western Interconnection).

12.6.2. Data Centers, Service Availability

Authorized vendors shall provide the same IaaS and PaaS cloud services (e.g., service catalog) from a minimum of two HA data centers.

12.6.2.1. Service Level Agreements

Authorized ordering entities are authorized to identify additional SLA requirements at the TO level.

12.6.3. Networking and Routing

12.6.3.1. Domain Network Service

Authorized vendors shall provide encrypted DNS that complies with OMB memo citation M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,* requirements.

12.6.3.2. Internet Protocol Access Control Lists (ACLs)

Authorized vendors shall provide a mean(s) and mechanism(s) that allows each IaaS and PaaS cloud services to be configured and managed using IP address ACLs (i.e., permit or deny access rules).

12.6.3.3. Internet Protocol Version 4

Authorized vendors may provide IPv4 accessibility to each IaaS and PaaS cloud services using IPv4 addresses (i.e., IPv4 compliant).

12.6.3.4. Internet Protocol Version 6

Authorized vendors shall provide IPv6 accessibility to each IaaS and PaaS cloud services using IPv6 addresses (i.e., IPv6 compliant).

12.6.3.5. Private and Public Subnets

Authorized vendors shall provide a mean(s) and mechanism(s) that allows each IaaS and PaaS cloud services to create, configure, and manage multiple private and public subnets.

12.6.3.6. Task Order(s), Networking and Routing

Authorized ordering entities are authorized to identify additional networking and routing requirements at the TO level.

12.7. Sub-Pool 1-1 Unclassified Infrastructure as a Service, Platform as a Service

Sub-pool 1-1 shall be used by authorized ordering entities for cloud services (i.e., IaaS, PaaS) supporting unclassified assets and systems and containing unclassified data.

12.7.1. Acquisition Requirements

RESERVED

12.7.2. Business Requirements

RESERVED

12.7.3. Cybersecurity Requirements

RESERVED

12.7.3.1. Clearance Levels – Personnel

Authorized vendors' persons (e.g., employees, representatives, sub-contractors) with data access, logical access, or physical access to authorized vendors' cloud services (e.g., IaaS, PaaS, SaaS) shall have a minimum clearance of Tier 4 (T4) Non-Sensitive Public Trust Positions - High Risk.

12.7.3.2. Cloud Service Offerings, Impact Level

Authorized vendors shall only provide FedRAMP CSOs (i.e., IaaS, PaaS) with a FedRAMP Moderate or High IL authorization.

Authorized vendors shall only provide DCAS CSOs (i.e., IaaS, PaaS) with a DCAS 2, 4, or 5 IL authorization.

12.7.3.2.1. Task Order(s) Cloud Service Offerings, Impact Level

Authorized ordering entities shall identify their CSOs IL requirements (i.e., FedRAMP: Moderate, High, DoD: 2, 4, 5) at the TO level.

12.7.4. Environmental Requirements

RESERVED

12.7.5. Operational Requirements

RESERVED

12.7.6. Technical Requirements

12.7.6.1. Cloud Service Offerings, Service Model Classification

Authorized vendors shall only provide FedRAMP or DCAS authorized IaaS and PaaS CSOs.

12.7.6.2. Task Order(s) Technical Requirements

Authorized ordering entities are authorized to identify additional technical requirements at the TO level.

12.8. Sub-Pool 1-2 Classified Infrastructure as a Service, Platform as a Service

Sub-pool 1-2 shall be used by authorized ordering entities for cloud services (i.e., IaaS, PaaS) supporting classified assets and systems and containing classified data.

12.8.1. Acquisition Requirements

RESERVED

12.8.2. Business Requirements

RESERVED

12.8.3. Cybersecurity Requirements

RESERVED

12.8.3.1. Clearance Levels – Personnel

Authorized vendors' persons (e.g., employees, representatives, sub-contractors) with data access, logical access, or physical access to authorized vendors' cloud services (e.g., IaaS, PaaS, SaaS) shall have a minimum clearance of Tier 3 (T3) National Security Positions - Secret / Confidential Clearance.

12.8.3.2. Cloud Service Offerings, Impact Level

Authorized vendors shall only provide DCAS CSOs (i.e., IaaS, PaaS) with a DCAS 6 IL authorization.

12.8.3.2.1. Task Order(s) Cloud Service Offerings, Impact Level

Authorized ordering entities shall identify their CSOs IL requirements (i.e., DoD: 6) at the TO level.

12.8.4. Environmental Requirements

RESERVED

12.8.5. Operational Requirements

RESERVED

12.8.6. Technical Requirements

12.8.6.1. Cloud Service Offerings, Service Model Classification

Authorized vendors shall only provide FedRAMP or DCAS authorized IaaS and PaaS CSOs.

12.8.6.2. Task Order(s) Technical Requirements

Authorized ordering entities are authorized to identify additional technical requirements at the TO level.

13. Pool 2: Software as a Service

Will consist of awardees that provide Government identified Software as a Service (SaaS) solutions Acquisition Requirements.

13.1. Business Requirements

RESERVED

13.2. Cybersecurity Requirements

RESERVED

13.3. Environment Requirements

RESERVED

13.4. Operational Requirements

RESERVED

13.5. Technical Requirements

RESERVED

13.6. Sub-Pool 2-1

Sub-pool 2-1 shall be used by authorized ordering entities for cloud services (i.e., SaaS) supporting Enterprise Office Productivity Software as a Service assets and systems.

13.6.1. Acquisition Requirements

RESERVED

13.6.2. Business Requirements

RESERVED

13.6.3. Cybersecurity Requirements

RESERVED

13.6.4. Environment Requirements

RESERVED

13.6.5. Operational Requirements

RESERVED

13.6.6. Technical Requirements

RESERVED

13.7. Sub-pool 2-2

Sub-pool 2-2 shall be used by authorized ordering entities for cloud services (i.e., SaaS) supporting Customer Relationship Management (CRM) Software as a Service assets and systems.

13.7.1. Acquisition Requirements

RESERVED

13.7.2. Business Requirements

RESERVED

13.7.3. Cybersecurity Requirements

RESERVED

13.7.4. Environment Requirements

RESERVED

13.7.5. Operational Requirements

RESERVED

13.7.6. Technical Requirements

RESERVED

14. Pool 3: Cloud Related IT Professional Services

Consist of awardees that provide cloud professional services that support the adoption of migration to, governance of, or management of commercial cloud computing solutions.

14.1. Acquisition Requirements

RESERVED

14.2. Business Requirements

RESERVED

14.3. Cybersecurity Requirements

RESERVED

14.4. Environment Requirements

RESERVED

14.5. Operational Requirements

RESERVED

14.6. Technical Requirements

RESERVED

14.7. Sub-Pool 3-1

RESERVED

14.7.1. Acquisition Requirements

RESERVED

14.7.2. Business Requirements

RESERVED

14.7.3. Cybersecurity Requirements

RESERVED

14.7.4. Environment Requirements

RESERVED

14.7.5. Operational Requirements

RESERVED

14.7.6. Technical Requirements

RESERVED

Appendix A: Abbreviations and Acronyms

Abbreviations & Acronyms		Expansion
A		
	A&A	Assessment & Authorization
	ACA	Associate Contractor Agreements
	ACO	Administrative Contracting Officer
	ACL	Access Control List
	AES	Advanced Encryption Standard
	AOR	Area of Responsibility
	API	Application Programming Interface
	ATO	Authorization To Operate
	AV	Audio Visual
B		
	BCAP	Boundary Cloud Access Point
	BI	Background Investigation
	BIC	Best In Class
	BPA	Blanket Purchase Agreement
	BYOD	Bring Your Own Device
C		
	CaC	Configuration as Code
	CAP	Cloud Access Point
	CCP	Common Catalog Platform
	CDM	Continuous Diagnostic and Mitigation
	CDO	Chief Data Officer

	CFE	Carbon Pollution-Free Electricity
	CFR	Code of Federal Regulations
	CIA	Confidentiality, Integrity, and Availability
	CISA	Cybersecurity and Infrastructure Security Agency
	CISCP	Cyber Information Sharing and Collaboration Program
	CISO	Chief Information Security Officer
	CLIN	Contract Line Item
	CMLC	Category Management Leadership Council
	CO	Contracting Officer
	CONUS	Continental United States
	COR	Contracting Officer Representative
	COTS	Commercial Off The Shelf
	CPARS	Contractor Performance Assessment Reporting System
	CPU	Central Processing Unit
	CS	Contracting Specialist
	CSO	Cloud Service Offering
	CSP	Cloud Service Provider
	CSV	Comma Separated Values
	CTA	Contractor Team Arrangements
	CUI	Controlled Unclassified Information
	CVD	Coordinated Vulnerability Disclosure
	CVE	Cybersecurity Vulnerability and Exposure
	CVS	Central Verification System
	CY	Calendar Year
D		

	DARP	Data At Rest Protection
	DB	Database
	DC	District of Columbia
	DC3	Department of Defense Cyber Crime Center
	DCAS	Department of Defense Cloud Authorization Services
	DCISE	Defense Industrial Base Collaborative Information Sharing Environment
	DCSA	Defense Counterintelligence and Security Agency
	DEL	Deliverable
	DFARS	Defense Federal Acquisition Regulation Supplement
	DHS	Department of Homeland Security
	DIB	Defense Industrial Base
	DISA	Defense Information Systems Agency
	DISC	Discount
	DISS	Defense Information System for Security
	DoD	Department of Defense
	DoD CC SRG	Department of Defense Cloud Computing Security Requirements Guide
	DoDD	Department of Defense Directive
	DoDI	Department of Defense Instruction
	DoDM	Department of Defense Manual
	DoJ	Department of Justice
	DoS	Department of State
	DOT&E	Office of the Director, Operational Test and Evaluation
	DSSR	Department of State Standardized Regulations
E		

	EDI	Electronic Data Interchange
	EOP	Executive Office of the President
	EPA	Environmental Protection Agency
	EPEAT	Electronic Product Environmental Assessment Tool
	ERO	Electric Reliability Organization
	etc	et cetera
F		
	FAR	Federal Acquisition Regulations
	FAQ	Frequently Asked Questions
	FBI	Federal Bureau of Investigations
	FCL	Facility Clearance
	FedRAMP	Federal Risk and Authorization Management Program
	FEMA	Federal Emergency Management Agency
	FFP	Firm-Fixed-Price
	FIPS	Federal Information Processing Standard
	FOC	Fiber Optic Cable
	FOUO	For Official Use Only
	FP	Fixed-Price
	FPU	Fixed Unit Price
	FSLT	Federal, State, Local, and Tribal
	FSS	Federal Supply Schedule
	FTR	Federal Travel Regulation
	FY	Fiscal Year
G		
	G&A	General and Administrative

	GAO	Government Accountability Office
	Gb	Gigabit
	GB	Gigabyte
	Gbps	Gigabits per second
	GEC	Global Electronics Council
	GFI	Government Furnished Information
	GFP	Government Furnished Property
	GOTS	Government Off The Shelf
	GSA	General Services Administration
	GSAM	General Services Acquisition Manual
	GUI	Graphical User Interface
H		
	HA	High Availability
	HHS	Health and Human Services
	HIPAA	Health Insurance Portability and Accountability Act
	HSPD	Homeland Security Presidential Directive
	HTTPS	Hypertext Transfer Protocol Secure
	HVAC	Heating, Ventilation, and Air Conditioning
I		
	IA	Information Assurance
	IaaS	Infrastructure as a Service
	IaC	Infrastructure as Code
	IAM	Identity and Access Management
	IAVA	Information Assurance Vulnerability Alert
	IAVM	Information Assurance Vulnerability Management

	IAW	In Accordance With
	IC	Intelligence Community
	ID	Identification
	IETF	Internet Engineering Task Force
	IL	Impact Level
	IM	Instant Messaging
	IPv4	Internet Protocol Version 4
	IPv6	Internet Protocol Version 6
	IRTPA	Intelligence Reform and Terrorism Prevention Act
	IS	Information Systems
	ISR	Industrial Security Representative
	IT	Information Technology
	ITC	Office of Information Technology Category
J		
	JPEG	Joint Photographic Experts Group
	JTR	Joint Travel Regulations
L		
	LH	Labor Hour
	LI-SaaS	Low Impact-Software as a Service
	LOA	Line of Accounting
M		
	MAC	Media Access Control
	MAS	Multiple Award Schedule
	MBI	Moderate Risk Background Investigation
	MFA	Multi-Factor Authentication

	MPEG	Moving Picture Experts Group
	MPIN	Marketing Partner Identification Number
	MRO	Midwest Reliability Organization
	MTIPS	Managed Trusted Internet Protocol Services
N		
	NA	Not Applicable
	NACI	National Agency Check and Inquiries
	NACLC	National Agency Check with Law and Credit
	NAICS	North American Industry Classification System
	NDA	Non-Disclosure Agreement
	NDAA	National Defense Authorization Act
	NERC	North American Electric Reliability Corporation
	NFHL	National Flood Hazard Layer
	NIST	National Institute of Standards and Technology
	NLT	No Later Than
	NPCC	Northeast Power Coordinating Council
	NSA / CSS	National Security Agency / Central Security Service
	NSS	National Security System
	NVD	National Vulnerability Database
O		
	O&M	Operations and Maintenance
	OCO	Ordering Contracting Officer
	OCONUS	Outside Continental United States
	ODNI	Office of the Director of National Intelligence
	OEM	Original Equipment Manufacturer

	OFPP	Office of Federal Procurement Policy
	OIG	Office of Inspector General
	OLM	Order-Level Materials
	OMB	Office of Management and Budget
	OS	Operating System
	OTP	One-Time Password
P		
	PA	Provisional Authority
	PaaS	Platform as a Service
	PHE	Public Health Emergency
	PII	Personally Identifiable Information
	PIV	Personal Identity Verification
	PMO	Program Management Office
	POA&M	Plan of Action and Milestones
	POC	Point of Contact
	PoP	Period of Performance
	PPD	Presidential Policy Directive
	PSC	Product Service Code
	PVC	Polyvinyl Chloride
	PWS	Performance Work Statement
Q		
	QTR	Quarter
	QTY	Quantity
R		
	R2	Responsible Recycling Standards for Electronic Recyclers

	RAM	Random Access Memory
	RF	ReliabilityFirst
	RFC	Request for Comment
	RM	Risk Management
S		
	SaaS	Software as a Service
	SAM	System for Award Management
	SAT	Simplified Acquisition Threshold
	SCIF	Sensitive Compartmented Information Facility
	SCR	Service Contract Reporting
	SCRM	Supply Chain Risk Management
	SEC	Securities and Exchange Commission
	SERC	SERC Reliability Corporation
	SIN	Special Item Number
	SKU	Stock Keeping Unit
	SLA	Service Level Agreement
	SLTT	State, Local, Tribal, or Territorial
	SMS	Short Message Service
	SOC	Security Operations Center
	SOO	Statement of Objectives
	SOW	Statement of Work
	SP	Special Publication
	SSBI	Single Scope Background Investigation
	Sub-CLIN	Sub-Contract Line Item
	SUM	Spend Under Management

T		
	T&C	Terms and Conditions
	T&M	Time and Materials
	TBD	To Be Determined
	TIC	Trusted Internet Connection
	TDR	Transactional Data Reporting
	Texas RE	Texas Reliability Entity
	TLS	Transport Layer Security
	TO	Task Order
	TOA	Task Order Award
U		
	U.S.C	United States Code
	UC	Unified Communications
	UN	United Nations
	UPC	Universal Product Code
	UPS	Universal Power Supply
	URL	Uniform Resource Locator
	US	United States (of America)
	USA	United States Army
	USAF	United States Air Force
	USG	United States Government
	USMC	United States Marine Corps
	USN	United States Navy
	US-CERT	United States-Computer Emergency Readiness Team
V		

	vCPU	virtual Central Processing Unit
	VOIP	Voice Over Internet Protocol
	VPAT™	Voluntary Product Accessibility Template
	VPP	Verified Products Portal
	VTC	Video Teleconference
W		
	WECC	Western Electricity Coordinating Council
	W3C	World Wide Web Consortium
X		
	XML	Extensible Markup Language
Y		
Z		
	ZTA	Zero Trust Architecture
0		
1		
2		
	24x7x365	24 hours a day, 7 days a week, and 365 days
3		
4		
5		
6		
7		
8		
9		

Appendix B: Definitions

Term	Definition
Active Service	A cloud service (i.e., IaaS, PaaS, SaaS) that has been allocated resources and is in an active performance state (i.e., actively performing work).
BPA Contracting Officer	A Contracting Officer that is responsible for the administration of the BPA.
Authorized Ordering Entity	An authorized ordering entity is a federal, state, or local government agency or other eligible entity that is authorized to use the GSA MAS FSS.
Authorized Reseller	An authorized reseller is an entity that has been explicitly authorized (e.g., contractual agreement) by a CSP(s) to act as an authorized agent or intermediary (e.g., cloud broker) to offer, negotiate, and sell, on the behalf of the CSP(s), the CSP's cloud services.
Authorized Vendor	An authorized vendor is an entity that has been awarded a BPA award by the BPA Contracting Officer. An authorized vendor can be either a CSP or an authorized reseller.
Broad Network Access[111]	Cloud services are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
Carbon Pollution-Free Electricity[112]	Electrical energy produced from resources that generate no carbon emissions, including marine energy, solar, wind, hydrokinetic (including tidal, wave, current, and thermal), geothermal, hydroelectric, nuclear, renewably sourced hydrogen, and electrical energy generation from fossil resources to the extent there is active capture and storage of carbon dioxide emissions that meets EPA requirements.
Cloud Service Provider	A CSP is an entity that directly operates and manages the cloud services (i.e., IaaS, PaaS, SaaS) technology (e.g., facility, hardware, software).

[111] NIST, SP 800-145: The NIST Definition of Cloud Computing, Essential Characteristics
[112] Executive Order 14057: Clean Energy Industries and Jobs; Efforts to Catalyze Through Federal Sustainability

Cloud Service Provider Account	An account that Is the primary, master, or root account that establishes the cloud services (i.e., IaaS, PaaS, SaaS) business, operational, and management relationship (e.g., on-demand self-service, measured services) between the authorized vendor (i.e., CSP, authorized reseller) and the authorized ordering entity.
Cloud Service	(Still To Do)
Cloud Service Offering	(Still To Do)
Commercial Item	(Still To Do)
Commercial Service	(Still To Do)
Cost Allocation	Cost allocation is the process of identifying, aggregating, and assigning costs to cost objects. A cost object is any activity or item for which you want to separately measure costs.
Community Cloud	(Still To Do)
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Hybrid Cloud	(Still To Do)
Infrastructure as a Service[113]	The capability provided to the authorized ordering entity to provision processing, storage, networks, and other fundamental computing resources where the authorized ordering entity can deploy and run arbitrary software, which can include operating systems and applications. The authorized ordering entity 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 (e.g., host firewalls).
Institution of Higher Education[114, 115]	An educational institution in any State that admits as regular students only persons having a certificate of graduation from a school providing secondary education, or the recognized equivalent of such a certificate; is legally authorized within such State to provide a program of education beyond secondary education; provides an

[113] NIST, SP 800-145: The NIST Definition of Cloud Computing, Service Models
[114] 40 U.S.C. 502(c)
[115] 10 U.S.C. 1001 EDUCATION, General definition of institution of higher education

	educational program for which the institution awards a bachelor's degree or provides not less than a 2-year program that is acceptable for full credit toward such a degree, or awards a degree that is acceptable for admission to a graduate or professional degree program, subject to review and approval by the Secretary; is a public or other nonprofit institution; and is accredited by a nationally recognized accrediting agency or association, or if not so accredited, is an institution that has been granted pre-accreditation status by such an agency or association that has been recognized by the Secretary for the granting of pre-accreditation status, and the Secretary has determined that there is satisfactory assurance that the institution will meet the accreditation standards of such an agency or association within a reasonable time
Law Enforcement	A law enforcement entity is an entity that has oversight (e.g., OIG) and / or law enforcement (e.g., DoJ, FBI, State Police) jurisdiction for the BPA Contracting Officer and / or authorized ordering entities.
Local Educational Agency[116, 117]	A board of education or other legally constituted local school authority having administrative control and direction of free public education in a county, township, independent school district, or other school district; and includes any State agency that directly operates and maintains facilities for providing free public education.
Measured Service[118]	Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the authorized vendor (i.e., CSP, authorized reseller) and the authorized ordering entity of the utilized service.
On-Demand Self-Service[119]	An authorized ordering entity can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each authorized vendor (i.e., CSP, authorized reseller).
Personally Identifiable	Refers to information which can be used to distinguish or

[116] 40 U.S.C. 502(c)
[117] Elementary and Secondary Education Act of 1965
[118] NIST, SP 800-145: The NIST Definition of Cloud Computing, Essential Characteristics
[119] NIST, SP 800-145: The NIST Definition of Cloud Computing, Essential Characteristics

Information	trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
Platform as a Service[120]	The capability provided to the authorized ordering entity to deploy onto the cloud infrastructure authorized ordering entity-created or acquired applications created using programming languages, libraries, services, and tools supported by the authorized vendor (i.e., CSP, authorized reseller). The authorized ordering entity 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.
Private Cloud	(Still To Do)
Public Cloud	(Still To Do)
Rapid Elasticity[121]	Cloud services can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the authorized ordering entity, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
Resource Pooling[122]	The authorized quoter's (i.e., CSP, authorized reseller) computing resources are pooled to serve multiple authorized ordering entities using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to authorized ordering entities' demand. There is a sense of location independence in that the authorized ordering entities generally have no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
Software as a Service[123]	The capability provided to the authorized ordering entity to

[120] NIST, SP 800-145: The NIST Definition of Cloud Computing, Service Models
[121] NIST, SP 800-145: The NIST Definition of Cloud Computing, Essential Characteristics
[122] NIST, SP 800-145: The NIST Definition of Cloud Computing, Essential Characteristics
[123] NIST, SP 800-145: The NIST Definition of Cloud Computing, Service Models

	use the authorized vendor'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 authorized ordering entity 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.
State or Local Government[124]	Includes any State, local, regional, or tribal government, or any instrumentality thereof (including any local educational agency or institution of higher education).
Suspended Service	A suspended service Is any cloud service (i.e., IaaS, PaaS, SaaS) that has been allocated resources but is in a paused performance state (i.e., not actively performing work).
Term Cloud Service	(Still To Do)
Terminated Service	A terminated service Is any cloud service (i.e., IaaS, PaaS, SaaS) that has been terminated and resources released.
Tribal Government[125]	The governing body of any Indian tribe, band, nation, or other organized group or community located in the continental United States (excluding the State of Alaska) that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians, and any Alaska Native regional or village corporation established pursuant to the Alaska Native Claims Settlement Act.

[124] 40 U.S.C. 502(c)
[125] 40 U.S.C. 502(c)

Appendix C: Deliverables Schedule and Milestones Dates, Blanket Purchase Agreement

Item No.	Deliverable/ Notification	Frequency	Due Date	Number of Copies/ Notifications	Medium/ Format	Submit to	Section Reference
01	Cybersecurity Assessment Annual Report	Annually	Within 30 days of completion of annual auditor assessment or recertification	One (1)	Electronic copy (via email)	BPA CO PM COR	5.1.1
02	C-SCRM Plan	Annually and/or As Required, when there is a change that affects one or more CNSSI 1253 security controls.	Within ten (10) business days of a change that affects one or more CNSSI 1253 security controls	One (1)	Electronic copy (via email)	BPA CO PM COR	
03	Evidence of current ISO Certifications	Varies	Within ten (10) business days of Certification Renewal	One (1)	Electronic copy (via email)	BPA CO PM COR	
04	Cybersecurity Incident Report Notification	Quarterly As Required, when there is a reportable incident	Within 72 hours of incident	One (1)	Electronic copy (via email)	BPA CO PM COR	
05	Cybersecurity Training Certification Report	Annually As Required, when new personnel onboard	Exactly one (1) year after date of award and every year thereafter during the five year period of performance Total of four (4)	One (1)	Electronic copy (via email)	BPA CO PM COR	7.0

			deliverables				
06	Earned Utilization Discount Report	Quarterly	Within 15 days from the last calendar day of each calendar year quarter (Mar, Jun, Sep, Dec)	One (1)	Electronic copy (via email)	BPA CO PM COR	11.5.2
07	Invoices	Monthly	Within 15 days from the last calendar day of the month	One (1)	Electronic copy (via email)	BPA CO PM COR	11.5.3.9
08	Services Summary Report	Annually	Exactly one (1) year after date of award and every year thereafter during the five year period of performance	One (1)	Electronic copy (via email)	BPA CO PM COR	11.5.7
09	Enhanced Transactional Data Report Vendors who have accepted the Schedule # 70 – Information Technology, Software & Services Solicitation FCIS-JB-980001B TDR MAS Modification may utilize their monthly SRP reporting process to comply with this	Monthly	Within 15 days from the last calendar day of the month If there was no order activity during the month, confirmation of no reportable data must be submitted within 30 calendar days of the last calendar day of the month.	One (1)	Electronic copy (via email)	BPA CO PM COR	11.5.8

	requirement provided that the additional data fields are required to be incorporated into this BPA.						
10	Key Personnel Roster Report	Initial As required, based upon personnel transition/departure	Within five (5) business days after BPA Award Within 10 business days of the last calendar day of the month	One (1)	Electronic copy (via email)	BPA CO PM COR	4.7

Appendix D: Example - Service Catalog

Cloud Services Catalog: ABC Worldwide										
BPA Pool / Sub-Pool	TO PoP	TO PoP Start Date	TO PoP End Date	CSP Name	Serv. Name	Serv. Description	Serv. Model	Auth. Entity	Impact Level	…
1-1	00	2022 01 01	2022 12 31	Cloud Inc.	Server Large	Server, 4 vCPU, 64 GB RAM, 25 Gbps	IaaS	FedRAMP	High	…
1-1	01	2023 01 01	2023 12 31	Cloud Inc.	Server Large	Server, 4 vCPU, 64 GB RAM, 25 Gbps	IaaS	DoD	2	…
2-1	02	2024 01 01	2024 12 31	Cloud Inc.	Cloud Viewer	Cloud security monitoring SaaS	SaaS	FedRAMP	Moderate	…

Cloud Services Catalog: ABC Worldwide - Continued										
Auth. Date	Disc. Date	CSP Identifier	Effective Price Date	Serv. Price	Unit of Meas.	EPEAT(™) Registered[126]	ENERGY STAR® Cert.[127]	SKU [128]	ZTA Pillar [129]	ZTA Comp[130]
2020 12 25	2030 12 25	UPC123	2021 12 01	$1.23 45	Comp / per Hour	Yes	Yes	SKU123	Infrastructure	
2021 12 25	2030 12 25	UPC123	2021 12 01	$1.23 45	Comp / per Hour	Yes	Yes	SKU456	Infrastructure	

[126] GSAM 552.238-78 Identification of Products that Have Environmental Attributes
[127] GSAM 552.238-78 Identification of Products that Have Environmental Attributes
[128] Optional Data Element.
[129] Optional Data Element.
[130] Optional Data Element.

2020 06 31	NULL	UPC456	2021 07 04	$0.02 50	Per Hour	No	Yes	SKUABC	Visibility and Analytics	Device Visibility

Appendix E: Example - Cloud Related IT Professional Services Catalog

Cloud Related IT Professional Services Catalog: ABC Worldwide									
BPA Pool / Sub-Pool	**TO PoP**	**TO PoP Start Date**	**TO PoP End Date**	**Professional Serv.**	**Professional Serv. Description**	**Clearance Level**	**Geo. Location**	**Place of Performance**	…
3-1	00	2022 01 01	2022 12 31	Cybersecurity Forensics	Services involved with processing, preserving, and analyzing computer-related evidence.	Tier 4 (T4) Non-Sensitive Public Trust Positions - High Risk	CONUS	Authorized Ordering Entity	**...**
3-1	00	2022 01 01	2022 12 31	Cybersecurity Forensics	Services involved with processing, preserving, and analyzing computer-related evidence.	Tier 3 (T3) National Security Positions - Secret / Confidential Clearance	CONUS	Authorized Ordering Entity	**...**
3-2	01	2023 01 01	2023 12 31	Ransomware Mitigation	Services involved with preventing, mitigating, and responding to malware attacks and infections.	Tier 3 (T3) National Security Positions - Secret / Confidential Clearance	GSA Region 5 Great Lakes	Authorized Ordering Entity	**...**
3-2	02	2024 01	2024 12	Ransomware	Services involved	Tier 3 (T3)	GSA	Authorized	**...**

		01	31	Mitigation	with preventing, mitigating, and responding to malware attacks and infections.	National Security Positions - Secret / Confidential Clearance	Region 9 Pacific Rim	Ordering Entity	
3-2	03	2025 01 01	2025 12 31	Ransomware Mitigation	Services involved with preventing, mitigating, and responding to malware attacks and infections.	Tier 3 (T3) National Security Positions - Secret / Confidential Clearance	GSA Region 11 National Capital	Authorized Ordering Entity	...

Cloud Related IT Professional Services Catalog: ABC Worldwide - Continued

Professional Serv. Code	Effective Price Date	Serv. Price	Unit of Meas	SKU[131]					
GSAU123	2021 12 31	$100.00	Hourly Rate	SKU001					
GSAC123	2021 12 31	$150.00	Hourly Rate	SKU002					
GSACR05RM	2022 07 04	$135.25	Hourly Rate	SKU003					

[131] Optional data element.

GSACR09RM	2022 07 04	$175.00	Hourly Rate	SKU004					
GSAUR11RM	2022 07 04	$145.50	Hourly Rate	SKU005					
GSACR11RM	2022 07 04	$185.75	Hourly Rate	SKU006					

Appendix F: Example - Fixed Price and Labor Hour Invoice

ABC Worldwide Invoice FP & LH									
BPA Award Num.	**TO Award Num.**	**TO PoP**	**TO PoP Start Date**	**TO PoP End Date**	**TO CLIN**	**TO Sub-CLIN**	**TO CLIN Type**	**Serv. Name**	**…**
01ABC123	02DEF456	00	2022 10 01	2023 09 30	0001	0001-A	FUP	Large Server	…
01ABC123	02DEF456	00	2022 10 01	2023 09 30	0002	0002-AB	FP	Cloud Viewer	…
01ABC123	02DEF456	00	2022 10 01	2023 09 30	0003	NULL	LH	Cybersecurity Forensics	…

ABC Worldwide Invoice FP & LH - Continued									
CSP Identifier / Prof. Serv. Code	**Serv. Start Date**	**Serv. End Date**	**Catalog Serv. Price**	**Serv. Price Disc.**	**TO Serv. Price**	**Unit of Meas.**	**QTY**	**Total Cost**	**SKU[132]**
UPC123	2022 11 01	2022 11 31	$1.2345	50%	$0.6173	Comp / per Hour	100	$61.73	SKU001
UPC456	2022 11 15	2022 11 31	$0.0250	NULL	$0.015	Hour	1000	$15.00	SKU002
GSAU123	2022 11 01	2022 11 31	$150.50	10%	$135.45	Labor Hour	100	$13,545.00	SKU003

[132] Optional data element.

Appendix G: Example - Time and Materials Invoice

ABC Worldwide Invoice T&M									
BPA Award Num.	**TO Award Num.**	**TO PoP**	**TO PoP Start Date**	**TO PoP End Date**	**TO CLIN**	**TO Sub-CLIN**	**TO CLIN Type**	**Serv. Name**	**…**
01ABC123	02DEF456	00	2022 10 01	2023 09 30	0002	0002-AA	T&M	Cybersecurity Forensics	…
01ABC123	02DEF456	00	2022 10 01	2023 09 30	ODC	NULL	T&M	Travel	…

ABC Worldwide Invoice T&M - Continued									
CSP / Prof. Serv. Code Unique Identifier	**Serv. Start Date**	**Serv. End Date**	**Catalog Serv. Price**	**TO Ceiling Price**	**Direct Costs**	**Indirect Costs**	**Fixed Handling Factor**	**Profit**	**…**
GSAU123	2022 11 01	2022 11 31	$250.00	$190.00	$75.00	$65.00	NULL	$25.00	…
NULL	2022 11 15	2022 11 18	NULL	NULL	$500.00	NULL	10%	NULL	…

ABC Worldwide Invoice T&M - Continued									
Unit of Meas.	**QTY**	**Total Cost**	**SKU**[133]						
Labor Hour	100	$16,500.00	SKU003						
Flight	1	$550.00	NULL						

[133] Optional data element.

Appendix H: Example - Services Summary Report

ABC Worldwide Services Summary Report									
BPA Award Num.	**TO Award Num.**	**TO PoP**	**TO PoP Start Date**	**TO PoP End Date**	**TO CLIN**	**Serv. Name**	**CSP / Prof. Serv. Code Unique Identifier**	**Average Serv. Utilization Rate**	**…**
01ABC123	02DEF456	00	2022 10 01	2023 09 30	0001	Large Server	UPC123	90%	…
01ABC123	02DEF456	00	2022 10 01	2023 09 30	0001	Large Server	UPC123	55%	…
01ABC123	02DEF456	00	2022 10 01	2023 09 30	0001	Load Balancing	UPC456	NULL	

ABC Worldwide Services Summary Report - Continued									
Unit of Meas.	**Cost Element**								**…**
Comp / per Hour	Cost								…
Comp / per Hour	Cost								…
NULL	No Cost								

Appendix I: Regulations, Policies, Specifications, Tools and References

— — Defense Federal Acquisition Regulation Supplement (DFARS)		
XX	DFARS 204.17 - Service Contract Inventory	https://www.acquisition.gov/dfars/part-204-administrative-and-information-matters#changeme_1626301504418
XX.1	DFARS 204.1703 Reporting Requirements	https://www.acquisition.gov/dfars/part-204-administrative-and-information-matters#DFARS_204.1703
F	DFARS 239.76 - Cloud Computing	https://www.acquisition.gov/dfars/part-239-acquisition-information-technology#DFARS-239.76
F.1	DFARS 239.7602-1 General	https://www.acquisition.gov/dfars/part-239-acquisition-information-technology#DFARS-239.7602-1
F.2	DFARS 239.7602-2 Required storage of data within the United States or outlying areas	https://www.acquisition.gov/dfars/part-239-acquisition-information-technology#DFARS-239.7602-2
XX	DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting	https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS-252.204-7012
	DFARS 252.227-7013 Rights in Technical Data—Noncommercial Items	https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS-252.227-7013
	DFARS 252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS-252.227-7014
	DFARS 252.227-7015 Technical Data–	https://www.acquisition.gov/dfars/pa

	Commercial Items	rt-252-solicitation-provisions-and-contract-clauses#DFARS-252.227-7015
	DFARS 252.227-7025 Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends	https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS-252.227-7025
	DFARS 252.239-7010 Cloud Computing Services	https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS-252.239-7010
— — Defense Information Systems Agency (DISA)		
	Memorandum 2019 08 15: Department of Defense (DoD) Memorandum of Reciprocity for FedRAMP Authorized Moderate Baseline Cloud Service Offerings (CSO) at Impact Level 2 (IL2)	Attachment X
— Department of State (DoS)		
	Standard Regulations	https://aoprals.state.gov/
— Executive Office of the President (EOP)		
L	Executive Order 13556: Controlled Unclassified Information	https://www.federalregister.gov/documents/2010/11/09/2010-28360/controlled-unclassified-information
M	Executive Order 14028: Improving the Nation's Cybersecurity	https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
XX	Executive Order 14035: Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce	https://www.federalregister.gov/documents/2021/06/30/2021-14127/diversity-equity-inclusion-and-accessibility-in-the-federal-workforce
N	Executive Order 14057: Clean Energy Industries and Jobs; Efforts To Catalyze Through Federal Sustainability	https://www.federalregister.gov/public-inspection/2021-27114/clean-energy-industries-and-jobs-efforts-to-catalyze-through-federal-sustainability-eo-14057
O	Homeland Security Presidential Directive	https://www.dhs.gov/homeland-

	12: Policy for a Common Identification Standard for Federal Employees and Contractors	security-presidential-directive-12
XX	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
XX	Presidential Policy Directive 41: Critical Infrastructure Security and Resilience	https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
— Federal Acquisition Regulation (FAR)		
XX	FAR 27.4 Rights in Data and Copyrights	https://www.acquisition.gov/far/part-27#FAR_Subpart_27_4
XX.X	FAR 27.404-1 Unlimited rights data	https://www.acquisition.gov/far/part-27#FAR_27_404_1
XX.X	FAR 27.404-2 Limited rights data and restricted computer software	https://www.acquisition.gov/far/part-27#FAR_27_404_2
XX	FAR 27.405-1 Special works	https://www.acquisition.gov/far/part-27#FAR_27_405_1
Q	FAR 31.205-46 Travel Costs	https://www.acquisition.gov/far/part-31#FAR_31_205_46
R	FAR 39.2 Information and Communication Technology	https://www.acquisition.gov/far/part-39#FAR_Subpart_39_2
XX	FAR 39.204 Exceptions	https://www.acquisition.gov/far/part-39#FAR_39_204
XX	FAR 39.205 Exemptions	https://www.acquisition.gov/far/part-39#FAR_39_205
U	FAR 52.204-14 Service Contract Reporting Requirements	https://www.acquisition.gov/far/part-52#FAR_52_204_14
V	FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems	https://www.acquisition.gov/far/part-52#FAR_52_204_21
W	FAR 52.227-14 Rights in Data-General	https://www.acquisition.gov/far/part-52#FAR_52_227_14
XX	FAR 52.227-17 Rights in Data-Special	https://www.acquisition.gov/far/part-

	Works	52#FAR_52_227_17
— — General Services Administration Manual (GSAM)		
Z	GSAM 552.216-75 Transactional Data Reporting	https://www.acquisition.gov/content/part-552-solicitation-provisions-and-contract-clauses#i1876737
XX	GSAM 552.238-78 Identification of Products that Have Environmental Attributes	https://www.acquisition.gov/gsam/part-552#GSAM_552_238_78
AA	GSAM 552.238-115 Special Ordering Procedures for the Acquisition of Order-Level Materials	https://www.acquisition.gov/content/part-552-solicitation-provisions-and-contract-clauses#i1876737
— Office of Management and Budget (OMB)		
BB	Federal Cloud Computing Strategy (Cloud Smart)	https://cloud.cio.gov/strategy/#cloud-smart
XX	M-16-12: Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing	https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2016
XX	M-19-13: Category Management: Making Smarter Use of Common Contract Solutions and Practices[134, 135]	https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2019
XX	M-21-07: Completing the Transition to Internet Protocol Version 6 (IPv6)	https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2021
XX	M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents	https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2021
XX	M-22-03: Advancing Equity in Federal Procurement	https://www.whitehouse.gov/omb/information-for-agencies/memoranda/#memoranda-2022
XX	M-22-09: Moving the U.S. Government	https://www.whitehouse.gov/omb/inf

[134] Best In Class, Spend Under Management, Tiered Maturity Model

[135] Portions of M-19-13: Category Management: Making Smarter Use of Common Contract Solutions and Practices have been revised by M-22-03: Advancing Equity in Federal Procurement

	Toward Zero Trust Cybersecurity Principles	ormation-for-agencies/memoranda/#memoranda-2022
— Office of the Director of National Intelligence (ODNI)		
XX	ICD 503: Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation	https://www.dni.gov/files/documents/ICD/ICD_503.pdf
— Specifications and Standards		
A	Standard for Responsible Recycling and Reuse of Electronic Equipment©	https://e-stewards.org/
B	Internet Engineering Task Force (IETF), RFC 8200, Internet Protocol, Version 6 (IPv6) Specification	https://datatracker.ietf.org/doc/html/rfc8200
XX	EPEAT Ecolabel	https://epeat.net/about-epeat
C	Responsible Recycling Standards for Electronic Recyclers (R2)	https://sustainableelectronics.org/welcome-to-r2v3/document-library/
D	EDI Standard Unit of Measure	https://x12.org
XX	FIPS PUB 197: Advanced Encryption Standard (AES)	https://csrc.nist.gov/publications/detail/fips/197/final
E	FIPS PUB 199: Standards of Security Categorization of Federal Information and Information Systems	https://csrc.nist.gov/publications/detail/fips/199/final
XX	FIPS PUB 201-3: Personal Identity Verification (PIV) of Federal Employees and Contractors	https://csrc.nist.gov/publications/detail/fips/201/3/final
XX	NIST, SP 500-267A Rev. 1: NIST IPv6 Profile	https://www.nist.gov/publications/nist-ipv6-profile
XX	NIST, SP 500-267B Rev. 1: USGv6 Profile	https://www.nist.gov/publications/usgv6-profile
XX	NIST, SP 500-292: NIST Cloud Computing Reference Architecture	https://www.nist.gov/publications/nist-cloud-computing-reference-architecture
XX	NIST, SP 800-37 Rev. 2: Risk Management Framework for Information	https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

	Systems and Organizations: A System Life Cycle Approach for Security and Privacy	
F	NIST, SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
XX	NIST, SP 800-63-3: Digital Identity Guidelines	https://csrc.nist.gov/publications/detail/sp/800-63/3/final
XX	NIST, SP 800-63A: Digital Identity Guidelines: Enrollment and Identity Proofing	https://csrc.nist.gov/publications/detail/sp/800-63a/final
XX	NIST, SP 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management	https://csrc.nist.gov/publications/detail/sp/800-63b/final
XX	NIST, SP 800-63C: Digital Identity Guidelines: Federation and Assertions	https://csrc.nist.gov/publications/detail/sp/800-63c/final
XX	NIST, SP 800-88 Rev. 1: Guidelines for Media Sanitization	https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
XX	NIST, SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing	https://csrc.nist.gov/publications/detail/sp/800-144/final
G	NIST, SP 800-145: The NIST Definition of Cloud Computing	https://csrc.nist.gov/publications/detail/sp/800-145/final
XX	NIST, SP 800-146: Cloud Computing Synopsis and Recommendations	https://csrc.nist.gov/publications/detail/sp/800-146/final
XX	NIST SP 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials	https://csrc.nist.gov/publications/detail/sp/800-157/final
H	NIST, SP 800-171 Rev.2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
XX	NIST, SP 800-171A: Assessing Security Requirements for Controlled Unclassified Information	https://csrc.nist.gov/publications/detail/sp/800-171a/final
XX	NIST, SP 800-172: Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171	https://csrc.nist.gov/publications/detail/sp/800-172/final

I	NIST, SP 800-181 Rev. 1: Workforce Framework for Cybersecurity (NICE Framework)	https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final
J	NIST, SP 800-190: Application Container Security Guide	https://csrc.nist.gov/publications/detail/sp/800-190/final
K	NIST, SP 800-207: Zero Trust Architecture	https://csrc.nist.gov/publications/detail/sp/800-207/final
L	NIST SP 800-210: General Access Control Guidance for Cloud Systems	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-210.pdf
XX	Web Authentication (WebAuthn)	https://www.w3.org/TR/webauthn-2/
— Information, References and Tools		
XX	Global Electronics Council	https://globalelectronicscouncil.org/
XX	EPEAT Registry	https://www.epeat.net/
XX	CVE(R) Program	https://cve.mitre.org/
North American Electric Reliability Corporation (NERC)		
A	Midwest Reliability Organization (MRO)	https://mro.net/
B	NERC	https://www.nerc.com
C	NERC Interconnections	https://www.nerc.com/AboutNERC/keyplayers/PublishingImages/NERC%20Interconnections.pdf
D	Northeast Power Coordinating Council (NPCC)	https://www.npcc.org/
E	ReliabilityFirst (RF)	https://rfirst.org/
F	SERC Reliability Corporation (SERC)	https://www.serc1.org/
G	Texas Reliability Entity (Texas RE)	https://www.texasre.org/
H	Western Electricity Coordinating Council (WECC)	https://www.wecc.org/
— Department of Defense (DoD)		
K	DoD Cloud Computing Security Requirements Guide (DoD CC SRG)	https://public.cyber.mil/dccs/dccs-documents/

L	DoD Cloud Strategy	https://dodcio.defense.gov/Library/
O	DoD Outside the Continental United States (OCONUS) Cloud Strategy	https://dodcio.defense.gov/Library/
P	DoD Zero Trust Reference Architecture	https://dodcio.defense.gov/Library/
M	DoDD 8140.01 Cyberspace Workforce Management	https://www.esd.whs.mil/Directives/issuances/dodd/
XX	DoDI 8500.01: Cybersecurity	https://www.esd.whs.mil/Directives/issuances/dodi/
XX	DoDI 8510.01: Risk Management Framework (RMF) for DoD Information Technology (IT)	https://www.esd.whs.mil/Directives/issuances/dodi/
XX	DoDI 8582.01: Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information	https://www.esd.whs.mil/Directives/issuances/dodi/
N	DoDM 8570.01-M Information Assurance Workforce Improvement Program	https://www.esd.whs.mil/Directives/issuances/dodm/
XX	Office of the Director, Operational Test and Evaluation	https://www.dote.osd.mil
XX	US Cyber Command	https://www.cybercom.mil/
— — Defense Counterintelligence and Security Agency (DCSA)		
Q	Central Verification System (CVS)	https://www.dcsa.mil/is/cvs/
R	Defense Information System for Security (DISS)	https://www.dcsa.mil/is/diss/
S	Facility Clearance	https://www.dcsa.mil/mc/ctp/fc/
— — Defense Information Systems Agency (DISA)		
T	DISA	https://disa.mil/
— — — Department of Defense Cloud Authorization Services (DCAS)		
U	DCAS Authorized Commercial Cloud Services	https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/cloud-service-support
— — Department of Defense Cyber Crime Center (DC3)		
XX	DC3	https://www.dc3.mil/

XX	Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE)	https://www.dc3.mil/Organizations/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/
XX	Defense Industrial Base (DIB) Cybersecurity (CS) Program	https://dibnet.dod.mil/portal/intranet/
XX	Defense Industrial Base (DIB) Cyber Reports	https://dibnet.dod.mil/portal/intranet
— — Cybersecurity & Infrastructure Security Agency (CISA)		
Y	AMAC Malware Analysis Submissions	https://www.malware.us-cert.gov
Z	Continuous Diagnostic and Mitigation Program	https://www.cisa.gov/cdm
AA	Coordinated Vulnerability Disclosure Program	https://www.cisa.gov/coordinated-vulnerability-disclosure-process
XX	Cyber Information Sharing and Collaboration Program (CISCP)	https://www.cisa.gov/ciscp
BB	Cyber Threat Indicator and Defensive Measure Submission System	https://us-cert.cisa.gov/forms/share-indicators
CC	EINSTEIN	https://www.cisa.gov/einstein
DD	Incident Reporting System	https://us-cert.cisa.gov/forms/report
XX	Moving the U.S. Government Toward Zero Trust Cybersecurity Principles	https://zerotrust.cyber.gov/
EE	Trusted Internet Connections	https://www.cisa.gov/trusted-internet-connections
XX	US-CERT	https://www.cisa.gov/uscert/
XX	US-CERT Federal Incident Notification Guidelines	https://www.cisa.gov/uscert/incident-notification-guidelines
— Environmental Protection Agency (EPA)		
HH	Certified Electronic Recyclers	https://www.epa.gov/smm-electronics/certified-electronics-recyclers
II	ENERGY STAR®	https://www.energystar.gov/
JJ	ENERGY STAR®, Data Centers	https://www.energystar.gov/products/data_centers

XX	Electronic Product Environmental Assessment Tool (EPEAT)	https://www.epa.gov/greenerproducts/electronic-product-environmental-assessment-tool-epeat
— Federal Risk and Authorization Management Program (FedRAMP)		
KK	FedRAMP	https://www.fedramp.gov/
LL	FedRAMP Marketplace	https://marketplace.fedramp.gov/
— General Services Administration (GSA)		
MM	Contractor Performance Assessment Reporting System (CPARS)	https://www.cpars.gov/
XX.X	Guidance for the Contractor Performance Assessment Reporting System (CPARS)	https://www.cpars.gov/help.htm
NN	Cooperative Purchasing Program	https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedule/schedule-buyers/state-and-local-governments/cooperative-purchasing
OO	Disaster Purchasing Program	https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedule/schedule-buyers/state-and-local-governments/state-and-local-disaster-purchasing
PP	eOffer / eMod	https://eoffer.gsa.gov/
QQ	Order Level Materials (OLM)	https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedule/schedule-features/orderlevel-materials-olms
RR	Public Health Emergencies Program	https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedule/schedule-buyers/state-and-local-governments/public-health-emergencies-program
SS	Transaction Data Reporting (TDR)	https://vsc.gsa.gov/TDR/
TT	Verified Products Portal (VPP)	www.gsa.gov/vpp
UU	Zero Trust Architecture (ZTA) Buyer's Guide Version 1.0 June 2021	https://www.gsa.gov/cdnstatic/Zero%20Trust%20Architecture%20Buyers%20Guide%20v11%2020210610%20(2).pdf

— National Archives		
WW	Controlled Unclassified Information (CUI)	https://www.archives.gov/cui
XX	Controlled Unclassified Information (CUI) Markings List	https://www.archives.gov/cui/registry/category-marking-list
— National Institute of Standards and Technology (NIST)		
XX	National Vulnerability Database (NVD)	https://nvd.nist.gov/
XX	USGv6 Program	https://www.nist.gov/programs-projects/usgv6-program
— National Security Agency / Central Security Service (NSA / CSS)		
XX	National Security Agency	https://www.nsa.gov/
XX	NSA Cybersecurity Collaboration Center	https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/
— System for Award Management (SAM)		
XX	System for Award Management (SAM.gov)	https://sam.gov/
XX	Service Contract Reporting (SCR)	https://sam.gov/content/entity-reporting
— Section508.gov		
XX	Section508.gov	https://www.section508.gov/
YY	Sell Accessible Products and Services	https://www.section508.gov/sell/
ZZ	Voluntary Product Accessibility Template (VPAT(™))	https://www.section508.gov/sell/vpat