U.S. Department of Homeland Security

Office of the Chief Information Officer

ATTACHMENT J-2: Performance Work Statement

for

Data Center and Cloud Optimization

February 2021

AMENDMENT 0005

Revision 2.0

This page intentionally left blank

1 General

The Department of Homeland Security (DHS) Data Center and Cloud Optimization (DCCO) acquisition plans to acquire information technology services to manage and operate the DHS Hybrid Computing Environment (HCE). The HCE is a collection of enterprise computing resources including a data center, colocation sites, and commercial and private cloud services. In addition, DHS will acquire associated professional services to automate, optimize, and modernize the HCE.

1.1 Background

The main source of enterprise computing resource for DHS has been Data Center 1 (DC1), a Government Owned Contractor Operated data center located at the National Aeronautics and Space Administration (NASA) Stennis Space Center in Mississippi. NASA owns and manages the data center facility. DHS is one among several tenants within this facility. DHS leases approximately 36,000 square feet of raised floor space in the data center. NASA provides power management, raised floor space, physical security, office space, environmental control, and fire suppression to support DHS IT needs.

In addition to DC1, DHS will add Infrastructure as a Service (IaaS) offered by Cloud Service Providers (CSPs) and colocation facilities to its portfolio of enterprise resources. The Contractor shall operate, optimize, and automate the HCE as an integrated entity. The addition of colocation and CSP environments will extend the capacity, scalability, and redundancy of DHS enterprise computing capacity by providing additional physical, virtual, and cloud resources.

As of September 2020, the operating environment for DC1 can be characterized by the following:

- 14 DHS Components hosting systems in DC1
- 109 Hosted customer Federal Information Security Modernization Act (FISMA) systems
- 2009 Physical servers; 1660 virtual machines (VM)
- Installed networking devices:174 Firewalls; 74 Load balancers; 46 Routers; 1,183 Switches
- 601 Racks populated with DHS equipment, 975 racks installed, total rack capacity 1049
- 765 Terabytes (TB) of provisioned storage, 432 TB utilized
- 7,267 Devices installed supporting Component-owned systems
- 1,425 Devices installed supporting data center management and operations
- Monthly workload statistics, January through June 2020
    - 2,694 Service desk tickets generated, ranging from 2,467 low to 2,940 high
    - 264 Change requests processed, ranging from 225 low to 288 high
    - 4,062 Incidents managed, ranging from 2,488 low to 7,395 high

Three unclassified General Support Systems (GSS) operate in DC1 that are essential for the management and operation of the current DC1 and the future HCE:

1. Data Center 1 (DC1) is the GSS providing the underlying hardware infrastructure for the data center consisting of hardware switches, routers, network devices, firewalls, load balancers, and WAN optimization appliances and respective operating systems for the data centers.
2. Data Center 1 Management Zone (DC1 MGTZN) is the GSS providing the support mechanism (management, monitoring, and storage) for DC1 systems consisting of the appliances, hardware (e.g., Storage Area Network (SAN) storage, storage hardware, encryption devices, tape libraries, tape backups, servers, blades, network devices, monitoring appliances), software, and applicable reporting mechanisms and enterprise solutions dedicated to supporting the availability of DC1 Component systems and services.
3. Infrastructure as a Service - DC1 (IaaS-DC1) is the GSS providing compute IaaS private cloud for production and development activities for DHS on-premises systems and applications. The support system provides virtualized networking, storage, and compute capacity and excludes platform as a service (PaaS). The system consists of a fabric manager, computing system chassis, blade servers, hypervisors, Cisco Unified Computing System (UCS) managers, and management tools.

The current HCE contains physical compute servers organized into five zones in DC1 and colocation facilities. The servers include but are not limited to x86 blades from HP, Dell, and other vendors. Server operating systems include but are not limited to Windows, Red Hat Enterprise Linux (RHEL), Community Enterprise Operating System Linux distribution (CentOS), and IBM Advanced Interactive eXecutive (AIX). Some of the servers are configured with hypervisors, including VMware and IBM Power Virtualization Center (VC), to provide VMs. Citrix products are used to support virtual desktop environments provided by the HCE. The HCE also contains storage servers and SANs including but not limited to products from EMC and Hitachi.

This requirement focuses on information technology services required to support the DHS HCE including those DC1 support services not provided by NASA and infrastructure support services at colocation sites. It also includes the migration, operation and maintenance of systems and applications among the data center, colocation, and cloud environments that constitute the HCE. For DC1, the DHS Federal Data Center Operations team coordinates with the NASA team for all facility support activities. DHS Federal staff act as the intermediary between NASA and the data center support services Contractor.

The purpose of this requirement is to acquire Contractor support for the operation, maintenance, automation, optimization, and modernization of the DHS HCE and to offer an efficient, responsive Information Technology (IT) hosting environment that serves as the foundation for continued computing operations in support of the DHS mission. The HCE shall include unclassified and classified IT infrastructure, applications, and data.

The Contractor shall provide data center-based hosting and IaaS obtained from both CSP commercial services and CSP services hosted in Government cloud approved environments. The

Contractor shall provide professional services to support application operation, migration, and Operations and Maintenance (O&M) Orders. The Contractor shall provide customer service including an introduction to HCE environments and services for DHS customers.

DHS intends to operate the HCE as a high priority 24x7x365 computing environment supporting critical mission and business needs for the Department. This includes, but is not limited to, maintaining Service Level Agreements (SLAs) and having the appropriately cleared and qualified staff and support services necessary to maintain operations.

The HCE will offer a more efficient, responsive IT hosting environment that serves as the foundation to ensure continued operations in support of the DHS mission.

1.2 Scope

The scope of this Performance Work Statement (PWS) is the provision of operations, hosting and professional services for the DHS HCE. The Contractor shall identify, provide and manage personnel, processes, tools, and reporting to facilitate transparency and decision-making as well as to support the transition to the future state HCE. This requirement also includes the continuing support of current operations and services.

The Contractor's responsibility within DC1 includes the maintenance, operation, enhancement and organization of the IT infrastructure technologies in the HCE. Power, environmental controls, and facility modifications come under the purview of NASA Shared Services Center (NSSC) National Center for Critical Information Processing and Storage (NCCIPS) management. Facility management for DC1 is out of scope in this PWS; provision of facility services in colocation environments is in scope.

The subject PWS will support a single award Indefinite-Delivery Indefinite-Quantity (IDIQ) Contract, which will be available for the use by only the DHS and its Components. All resulting requirements anticipated for execution under this IDIQ Contract shall be coordinated through the Office of the Chief Information Officer (OCIO) Directorate of Information Technology Operations (ITO) Enterprise Operations Division (EOD).

1.3 Objectives

The DCCO requirements will be the core support services needed to drive a more efficient, responsive hybrid IT environment that serves as the foundation for the management and integration of on-premises, colocation, and cloud-based environments.

These support services must optimize and ensure continued DC1 operations while implementing and managing the future state HCE in support of the DHS mission and, where appropriate, the migration of infrastructure and applications within the HCE (e.g., from DC1 to CSP environments).

The objective of DHS's DCCO support service is to expedite the transformation of IT capabilities from an asset-based model to a service-based, customer-centric IT business model; provide transparent operational expenditures; and reduce both capital expenditures and time-to-delivery for new capabilities. To accelerate this transformation, DHS will continue existing initiatives associated with cloud optimization efforts as well as leverage new approaches. The business objectives for this requirement include:

1. Improved Total Cost of Ownership (TCO) and Cost Transparency - Continuously improve the operation of the HCE and provide detailed operational and financial metrics to guide improvements.
2. Modernization and optimization - Operations within the HCE should reflect state-of-the-art, optimized, automated, modern processes that rely upon automatic processes, to the maximum extent practicable, with the minimum required human intervention.
3. Responsiveness - Maximize the customer experience, improve trust, reduce the time to deliver, and enhance operational performance.
4. Scalability - Elastically scale hosting environments and supporting services quickly to meet mission operations and surge capabilities.
5. Improved Reliability and Availability - Monitor and improve Mean-Time-Between-Failures and Mean-Time-To-Repair metrics.
6. Secure HCE Environment - Monitor and evaluate systems, capabilities, interfaces, applications and data transactions to assess and mitigate cybersecurity threats.
7. Continual Operational Assessment and Improvement - Continuously collect and analyze performance metrics - both technically and administratively - to identify and implement optimizations that improve products and services, and processes reflected by those metrics - leading to continuing performance improvements as processes achieve greater levels of optimization.
8. Architectural approach - Identify objectives for further development and improvement of the HCE technical architecture that enhance interoperability, improve standards, reduce risks, improve security, and support the ability of DHS to take advantage of emerging technologies and capabilities.
9. Service Governance - Enforce a strong governance mechanism to ensure consistent interpretation of policy, monitor DHS enterprise computing performance, adhere to DHS policy requirements and address stakeholder issues.
10. Simplified Management - Improve communication through a data-driven, transparent, management approach that allows for clear focus and attainment of management and technical goals.

1.4 Applicable Documents

See Appendix A for a full list of Applicable Documents.

1.5 Performance Requirements Summary

This PWS includes a Performance Requirements Summary (PRS) in Section 12. The PRS plays an integral role in the administration of the resulting contract. In addition to any applicable inspection clauses or other related terms and conditions contained in the contract, the PRS shall serve as a primary tool for inspection and acceptance of services as facilitated by the Contracting Officer's Representative (COR). Evaluation of the Contractor's overall performance shall be in accordance with the performance standards set forth in the PRS, and will be conducted by the

COR. The PRS constitutes a material aspect of the PWS and will not be changed or otherwise modified without prior written approval of the Contracting Officer.

1.6 Definitions

Incident Severity. Categorization of the level of negative impact that service outages have on the DHS enterprise.

a. *Severity 1* - production systems or applications either not operating or unavailable causing end users to be unable to work in a single or multiple sites for one or more DHS Components.
b. *Severity 2* - development environments unavailable with no workaround or alternate with intermittent or no functionality for multiple users in a single or multiple sites for one or more DHS Components; or production environments operating in failover or redundancy mode with intermittent or no functionality for multiple users in a single or multiple sites for one or more DHS Components.
c. *Severity 3* - production systems or applications operating in failover or redundancy mode with no impact to multiple users in one or multiple sites for one or more Components; or testing, preproduction, or development environments operating in failover or redundancy mode with intermittent or no functionality for multiple users at one or multiple sites for a single Component.

Inventory. Inventory shall consist of a complete list of all equipment (i.e., hardware), applications (i.e., software), and resources within the HCE, in all physical, virtual, colocation and cloud environments. Software inventory parameters include but are not limited to applications, system, owner, software type, description, type of license (e.g., enterprise, single site), version, cost, date of acquisition, date of installation, and anticipated end of software assurance date.

2 Management Requirements and Tasks

The Contractor shall support the requirements in this Section across the HCE. The support includes physical and virtual assets in the DC1 facility in Stennis, MS. It includes the addition of private cloud assets in DC1 and in colocation facilities. The support also includes the addition of commercial cloud and Government cloud approved environment assets from CSPs. All these assets shall be considered as part of the HCE.

2.1 DHS Information Technology Infrastructure Management

The Contractor shall manage DHS IT infrastructure. As required, the Contractor shall interface with DHS Data Center Operations Team to address any issues that require modification to general facility services. The Contractor shall be responsible for implementing operational best practices including the following:

- HCE Operations, Maintenance, and Management
- Network Communications LAN & WAN
- Governance
- Service Classification
- Hybrid Computing Environment Management Automation

- Policies and Procedures
- General Support Systems Management
- Customer Dashboard and Information Repository
- Acquisition
- Colocation Services
- Cloud Services Management
- Intermediary for Software Licenses
- Hardware and Software License Management System Architecture / Engineering
- Contract Transition
- Automation
- Evolving Technology Evaluation

2.1.1 HCE Operations, Maintenance, and Management

The Contractor shall operate, maintain, and manage the DHS HCE which includes DC1, colocation facility installations, and cloud resources. The Contractor shall operate the HCE on a 24x7x365 basis with at least 99.9% availability. Within the HCE the Contractor shall manage, maintain, and operate Component owned equipment, systems, and software as specified on Task Orders and the GSS described in Section 1.1. The HCE shall provide compute, storage, network, database, and security services for DHS and Component use. Storage services include file, object, block and archival storage. The Contractor shall work with the DHS Data Center Operations Team and COR for any facility management support.

The Contractor shall generate and maintain a Service Offering listing of all services provided within the HCE. The Contractor shall post the Service Offering listing in the Information Repository (See Section 2.1.8) and update the listing with changes as needed but not more than 30 days following actual changes to service offerings.

The Contractor shall meet with the COR and other Government Program representatives weekly to review performance and address operational and managerial issues.

2.1.2 Network Communications LAN & WAN

The Contractor shall maintain and operate Local Area Networks (LAN) within HCE facilities and environments that connect to the DHS Homeland Security Enterprise Network (HSEN) Wide Area Network (WAN) also known as OneNet. DHS provides all WAN connectivity points and equipment. The LAN shall provide dual ports to each hosted server for redundancy and an overall redundant architecture.

The Contractor shall monitor and administer network traffic throughout the HCE, forecast bandwidth requirements associated with service requests, and implement network modifications to accommodate demand. The Contractor shall design the network architecture to support networking requirements including provision for a Zero Trust model and maintain as-designed and as-installed architecture drawings and descriptions in the Information Repository. The Contractor shall also provide dashboard displays of real time network performance metrics and posts notices regarding unplanned network outages as well as any planned service disruptions.

The Contractor shall provide any access or network monitoring required by DHS management or programs and shall support any integration with enterprise monitoring requirements.

2.1.3 Governance

The Contractor shall operate under the umbrella of DHS governance and oversight processes that dictate interactions among DHS Headquarters, DHS Components, the Contractor Team, colocation providers, CSPs, and all other DHS contractors addressing interrelated requirements.

The Contractor shall adhere, follow, and support all DHS IT and Information Security Policy in governing change and configuration management.

The Contractor shall obtain Government approval for all solutions proposed to satisfy requirements and for all purchases required to fulfill those requirements.

2.1.4 Service Classification

The Contractor shall be capable of providing Level 1 services (see Section 3.8.1), Level 2 services (see Section 3.8.2), and Professional Services (see Section 4) at classified levels, Secret and Top Secret, at DC1 and at all current and future colocation facilities.

The Contractor shall provide services at the following classification levels across the HCE:

- Sensitive But Unclassified (SBU) Level. Including FedRAMP certified services from CSP commercial and CSP Government cloud approved environments assessed at FIPS 199 Low-Low-Low categorization, up to a High-High-High categorization, and variations of any FIPS 199 categorization.
- Secret Level. Services at the Secret level including services in Secret CSP environments.
- Top Secret (TS) / Sensitive Compartmented Information (SCI) Level. Services at the TS/SCI level including services in TS/SCI CSP environments.

This includes services from public CSPs and includes both commercial and Government cloud approved environments.

The Contractor shall provide services support for Sensitive Compartmented Information Facilities (SCIFs) in HCE in compliance with DHS and Government Security Directives, as needed.

DHS will provide agency specific guidance on the protection of national security information post award.

2.1.5 Hybrid Computing Environment Management Automation

The Contractor shall automate processes throughout the HCE to maximize operational efficiency, included but not limited to:

- Alert Monitoring
- Circuit Monitoring
- Change Management
- Incident Management
- CSP-based Monitoring

- Configuration Management
- Infrastructure, Security, and Network Monitoring
- Hardware and Software Monitoring
- Analytics, Intelligence, and Reporting

2.1.6 Policies and Procedures

The Contractor shall create, update, and maintain Contractor policies and procedures that govern its operation of the HCE and store those policies and procedures in the Information Repository described in Section 2.1.8.

2.1.7 General Support Systems

The Contractor shall manage, operate, and maintain the existing equipment, software, and other assets that constitute the GSS described in Section 1.1 to manage the existing HCE environment. The Contractor shall extend GSS management, operation, and maintenance capabilities beyond DC1 to all HCE resources, current and future. The Contractor shall provide dashboard access to GSS-generated reporting, metrics, and statistical data. The Contractor shall be responsible for populating various reports and interfacing GSS operational data to enterprise dashboards as requested.

The Government will provide the infrastructure currently in place supporting the three GSS listed in Section 1.1 as Government Furnished Equipment (GFE). The Contractor shall assume full responsibility for maintaining, enhancing, updating, and operating the hardware and software included within that infrastructure so that the Contractor meets the Government performance requirements. As equipment upgrades, technical refreshments, and replacements are required, the Contractor shall accomplish those upgrades, refreshments, and replacements with hardware and software purchased and owned by the Contractor. DHS intends to transition the three GSS systems described in Section 1.1 from Government Owned, Contractor Operated status to Contractor Owned, Contractor Operated during the period of performance of this contract. This transition will be executed through task order(s) under this IDIQ.

The Government will provide the list of GFE and any related information regarding the GSS listed in Section 1.1 as specified in Section 8.

The Contractor shall support and provide continuous availability of Workplace as a Service (WPaaS) private cloud service supported by the IaaS-DC1 GSS system described in Section 1.1. WPaaS provides virtualized desktops that are accessible by all DHS Components subscribing to the service.

2.1.8 Customer Dashboard and Information Repository

The Contractor shall develop, establish, maintain, and operate one or more centralized, integrated dashboards and a centralized Information Repository with real-time, on-demand, 24x7x365 access by DHS and Components. The Contractor shall provide role-based access to authorized DHS users and groups, with privileges allowing viewing, data retrieval, and data download in formats (e.g., Microsoft EXCEL, PDF) suitable for analytical processing.

The Contractor shall use the dashboard to track and manage assets and services provisioned and consumed in the HCE, including DC1, colocation centers, and CSPs. The dashboards shall

enable DHS to manage, use, report, audit, and track assets and services. The dashboards shall include inventory and management of physical and virtual assets and cloud services, usage and performance metrics for all assets and services, security metrics such as cyber threats and vulnerabilities, and metrics for billing and accounting. The dashboards shall capture and report actual and anticipated expenditures, purchases from the catalogs established under this contract, and forecast future spending to support financial, budget, audit, and benchmarking activities. The dashboards shall also provide visibility into resource and asset tagging.

The Contractor shall implement a Financial Management solution based on ITIL Version 4 to provide cost-effective management of HCE resources in accordance with awarded Task Orders. The Contractor shall provide a dashboard displaying all spending and purchasing under awarded Task Orders and forecasts for future spending.

The Contractor shall establish a centralized knowledge management capability, in conjunction with the dashboard and Information Repository, to share deliverables and related documentation about the HCE. The Contractor shall populate the Repository with information and documentation during the Transition-in Period. The Contractor shall maintain current versions of all documentation during the contract performance period in the Repository and shall provide final versions during the Transition-Out period. The Contractor shall provide DHS with access to the information throughout the period of performance.

The Contractor shall work with DHS to modify the Dashboard and the Information Repository as requested. The Contractor shall perform periodic quality assurance reviews on dashboard data to ensure accuracy and make necessary modifications. The Contractor shall ensure DHS can collect, analyze and synthesize the data (e.g., usage, security, performance) along with system metrics and SLA results on the services being provided. The Contractor shall also enable DHS to collect, analyze and synthesize cost data, including non-labor or professional services, to ensure accurate billing, configuration, and cost transparency. The Contractor shall enable dashboard data to be exported into formats, such as Microsoft Office and Adobe PDF for download.

The Contractor shall upload deliverables, work products, and related material to the Information Repository. These documents shall include environment descriptions and operations manuals, describing the HCE data center, colocation, and cloud IaaS environments, usage, processes and procedures, with updates when there are significant changes in those environments, processes or procedures. The Contractor shall provide separate addendums to these documents for customer unique configurations, processes, or procedures.

2.1.8.1 Real Time Resource Consumption and Cost Tracking

The dashboard shall enable DHS to use, track, report and audit all assets and services, including compute instances, storage volumes, and third-party products. The dashboard shall enable DHS to set and manage manual and automated approval of workloads, quotas, and thresholds for asset and service usage across the HCE for organizational and project-specific accounts. The dashboard shall enable DHS to provision, deploy, deprovision, and decommission assets, infrastructure, and services manually or automatically. The dashboard shall enable DHS to start, stop, terminate, and reboot virtual machines and services. The dashboard shall separate usage costs into billable groups for reporting purposes; and shall provide DHS with the ongoing capability to set thresholds and limits to usage, deployment, and provisioning of resources.

2.1.8.2 Catalog Purchase Tracking

The Contractor shall track all purchases made through the catalogs established under this contract for equipment & software, professional services, and cloud infrastructure as a service. The Contractor shall record each catalog's purchase transactions in a dashboard data set stored in a processable format available to the Government for review and download as part of the Monthly Financial report. The Contractor shall ensure that the purchase data set is updated monthly with notification to the Government upon completion.

2.1.8.3 Capacity Management

The Contractor shall monitor the capacity utilization of HCE resources and provide real-time dashboard displays and periodic reports to DHS regarding capacity utilization. The Contractor shall also develop future capacity requirement projections for each type of resource provided within the HCE. The contractor dashboard shall integrate with DHS enterprise-level systems and dashboards for data uploads, downloads, monitoring, and reporting.

2.1.9 Acquisition

Requirements may demand the acquisition of computing, communications, and data storage assets necessary to host and operate systems applications that DHS Components want to implement and operate. The Contractor shall assess the Task Order requirements specified by Components, determine whether resources are available within the HCE, and either allocate resources if available or procure additional resources as necessary to satisfy those requirements.

2.1.10 Colocation Services

The Contractor shall provide colocation services to DHS customers and shall support the process to obtain physical security authorization and Authority to Operate (ATO) at these colocation locations. Colocation services are defined as leased data center services that provide facility management, connectivity, cloud enablement, and security services. The Contractor shall provide the same operations, maintenance, and management services in colocation facilities as provided in DC1 including on-site hands-on services.

2.1.11 Cloud Services

The Contractor shall obtain CSP commercial cloud and Gov-Cloud IaaS and ancillary cloud services on behalf of DHS customers. The Contractor shall identify FedRAMP certified IaaS and ancillary cloud services offered by CSPs that meet DHS customers' technical, security, and business objectives as defined in Task Orders and subsequently acquire, integrate, and manage those services as components of the HCE on behalf of the Government.

2.1.12 Intermediary for Software Licenses

The Contractor shall purchase software licenses on behalf of DHS, manage all software licenses, and provide visibility of software licenses within the HCE.

2.1.13 System Architecture / Engineering

The Contractor shall provide system architecture and engineering services in order to maintain and continuously improve the HCE. The Contractor shall document the HCE system architecture including DC1, colocation centers, CSP infrastructure, the interconnections among HCE elements, and HCE security provisions. The Contractor shall develop and maintain associated operations manuals to optimize operations by DHS and store those architectural descriptions and manuals in the Information Repository.

2.1.14 Contract Transition

The Contractor shall assume responsibility for the management and operation of the HCE from the existing contractor and shall ensure that all operations continue with minimal to no disruption during the contract transition.

2.1.14.1 Transition-In

The Contractor shall develop and implement an Incoming Transition Plan to accomplish the transition of operations from the current service provider to the DCCO Contractor within 120 days from Transition Task Order award without any disruption of service. At a minimum, the Transition shall include:

1. Establishing a Contractor Transition Team within 5 business days of Task Order award.
2. Conducting and completing a site survey and assessment of DC1 within 15 business days of Task Order award.
3. Creating and delivering a draft contract-level Transition-In Plan for assuming full operational and management control of the HCE to include an initial staffing plan, within 30 business days of Transition-In Task Order award. The Contractor shall deliver a final Transition Plan, to include the final staffing plan, within 90 business days of Transition-In Task Order award.
4. Developing and implementing one or more dashboards as part of the Transition-In Task Order to achieve the objectives described in section 2.1.8. The Contractor shall incorporate costs associated with on-going dashboard operation, maintenance, and enhancement within its overall management cost structure.
5. Conducting and documenting an inventory of all equipment (i.e., hardware) and applications (i.e., software), and resources within the HCE - in all physical, virtual, colocation and cloud environments within 60 days of Task Order award.
6. Providing continuous operation of WPaaS, a private cloud service provided by IaaS-DC1.
7. Establishing Task Orders under this new contract for continuing existing customer data center support and Task Orders for new customer support requirements in the HCE. Task Order transition will be addressed on an order by order basis. All Task Orders under the predecessor contract all expire with that contract and must be established under the new contract.

2.1.14.2 Transition-Out

The Contractor shall:

1. Create and deliver an Exit Transition Strategy Plan within 60 days of Transition-in Task Order Award.
2. Deliver final updates on all policies and procedures governing current operations within the HCE not less than 90 days prior to the end of the period of performance or last exercised option period.
3. Deliver a current, final outgoing inventory of all equipment (i.e., hardware) and applications (i.e., software), and resources within the HCE - in all physical, virtual, colocation and cloud environments, not less than 90 days prior to the end of the period of performance or last exercised option period.

2.1.14.3 Task Order Transition Exit

Shall be specified at the Task Order Level.

2.1.15 Evolving Technology Evaluation

The Contractor shall track, research, and evaluate evolving and emerging technologies that have the potential to improve HCE operations through lower operational cost or improved technical performance and recommend improvements to the HCE to the Government. Those recommendations accepted by the Government will be reflected in subsequent Task Orders. The Contractor may incorporate new or emerging technologies within the three GSS described in Section 1.1 at the Contractor's discretion after DHS review and approval.

2.2 Security Services - HCE Level

The Contractor shall monitor the security of HCE components, and coordinate with DHS as appropriate, by performing the following work activities:

2.2.1 Security Operations Management

The Contractor shall provide security management services for the HCE and shall also provide specific security-related services in accordance with awarded Task Orders. The security services include maintenance of Zero Trust through identity and access management (role-based or attribute-based) with multifactor authentication and include encryption to protect data at rest and in transit. The contractor shall ensure any access requirements or security monitoring needed by DHS management or programs, or integration with enterprise monitoring requirements, is provided.

The Contractor shall implement the security controls required for DHS servers or applications and implement security mitigations as recommended by the Network Operations and Security Center (NOSC) or other enterprise-level authority. The Contractor shall conduct security testing to verify that the servers, applications, and networking and other equipment are protected against potential cyber threats.

Personnel security services are addressed in Section 5.5.2.

2.2.1.1 Vulnerability Assessments

The Contractor shall implement and deploy the tools, toolsets, and staff to support, operate, and maintain vulnerability assessment services in the HCE for systems and services delivered and operated by the Contractor. The Contractor shall develop a Vulnerability Assessment Plan and conduct routine, network-based vulnerability scans and assessments.

The Contractor shall track and collect threat and vulnerability data, report threats and vulnerabilities in the centralized dashboard, and implement mitigations as a defense from potential attacks.

2.2.1.2 Intrusion Detection and Prevention Systems (IDS/IPS)

The Contractor shall deploy, operate and maintain an Intrusion Detection System (IDS) to include host-based and network-based detection and an Intrusion Prevention System (IPS) to include host-based and network-based prevention for networks and systems resident within the HCE.

2.2.1.3 Firewall Management

The Contractor shall operate and maintain firewall software and hardware components and implement and deploy the tools, toolsets, and staff to support, operate, manage and maintain firewalls for applications, systems, and services delivered and operated by the Contractor within the HCE.

2.2.1.4 Anti-Virus Management

The Contractor shall operate and maintain anti-virus protection for the HCE and ensure that signatures and databases are the latest approved and tested versions.

2.2.2 Equipment Access and Control

The Contractor shall:

1. Ensure that all delivery and removal of equipment within the data center facility is authorized by DHS personnel.
2. Ensure that Contractor-issued and owned electronic devices meet DHS configuration guidance, otherwise the equipment shall not be permitted in the data center.
3. Prevent personally owned electronic devices (e.g., laptops, portable storage media, cell phones, etc.) from being taken into restricted areas within the data center.
4. Scan all electronic devices (e.g., government-issued devices, and Contractor-furnished devices) to identify vulnerabilities, verify the existence of up-to-date virus definitions, and ensure compliance with DHS configuration and policy guidance.
5. Dispose of or destroy media containing sensitive information in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization and DHS Sensitive Systems Policy Directive 4300A*. Inventory tracking status and approval chain of custody shall be updated in the dashboard.

6. Allow the DHS-appointed Communications Security (COMSEC) custodian to execute the responsibilities as outlined in DHS National Security Systems Policy 4300B.200 (COMSEC) Version 4.0.

2.2.3 Authority to Operate

The Contractor shall obtain and maintain a formal ATO as described in the DHS System Authorization Guide for the three GSS described in Section 1.1.

2.2.4 Risk Management

The Contractor shall create a Risk Management Plan and conduct and document Risk Assessments (RA) for the GSS operated by the Contractor after completing a NIST 800-53 evaluation, Contingency Plan testing, and assisting the OCISO in conducting Security Tests and Evaluation (ST&E). Risk Assessments shall identify threats and vulnerabilities, assess the impacts of the threats, evaluate in-place countermeasures, and identify additional countermeasures necessary to ensure an acceptable level of security. Risk Assessments shall also address the cost and schedule of mitigation activities. The Contractor shall update Risk Assessments annually.

2.2.5 Common Controls

The Contractor shall:

1. Enter security controls for each GSS that the Contractor operates and for the infrastructure supporting DC1 private cloud service offerings and the HCE in the DHS Enterprise Cyber Risk Management tool, currently Xacta, and update those controls annually. The controls shall consist of controls provided by FISMA systems as well as physical controls inherited or provided by NCCIPS and by Contractor processes and services such as Change Management and anti-virus deployment.
2. Provide inheritable controls to be used by tenants for their security documentation for systems and applications that those tenants implement on the HCE and enter into the DHS Enterprise Cyber Risk Management tool. These tenant systems and applications will inherit the controls entered by the Contractor in the DHS Enterprise Cyber Risk Management tool for the private cloud infrastructure.
3. Provide additional security controls for systems and services delivered and operated by the Contractor.

2.2.6 Access Management

The Contractor shall provide DHS with full inquiry, retrieval, and data download user access to all approved service offerings. In addition to user access, the Contractor shall enable application access to the HCE by enterprise applications. This shall include allowing applications to use the Application Programming Interfaces (APIs), Management Consoles, and Software Development Kits (SDKs) available from the CSPs, to directly interact with CSP services.

3 Operations Support Requirements and Tasks

3.1 Operations Services

The Contractor shall provide HCE operations services on a 24x7x365 basis. The Contractor shall provide real-time system status to DHS customers and provide monthly service level reports. The Contractor shall develop and maintain Standard Operating Procedures (SOPs) governing infrastructure operations to align with relevant SLAs and shall provide access to the documentation following commercial and federal standards and best practices.

3.2 Service Desk

The Contractor shall maintain and operate a 24x7x365 Service Desk for infrastructure, applications, and services residing within the HCE. The Contractor shall respond to and manage incidents occurring within the HCE. The Contractor shall provide efficient management of incident response and maintain communication with DHS stakeholders during response and resolution and provide an escalation path for the resolution of complex issues. The Contractor shall:

1. Accept and process incoming service requests.
2. Track and manage service requests from receipt through closure, problem reports to closure, and provide statistics for service desk performance reporting and analysis.
3. Provide enterprise help desk support for GSS applications that the Contractor operates in on-premises locations, colocation environments, approved CSP platforms and environments, and internal private cloud infrastructure supported by the Contractor.
4. Provide service and incident management support to Components for systems, applications, and services hosted within the HCE.
5. Integrate solutions (e.g., service management software), processes, and procedures with overall DHS IT enterprise reporting solutions and incident management processes and functions as components of enterprise DHS incident management.
6. Provide documented root cause analysis on request with recommendations for remediation and provide initial and final analysis reports to DHS, load reports to the Information Repository, and provide role-based access to the root cause reports.
7. Track ongoing infrastructure operation metrics and Service Desk performance metrics in the dashboard, in the monthly Service Quality Review (SQR), and in the formal quarterly Service Level Agreement Level of Service Report.

3.3 Inventory Control and Asset Management

The Contractor shall use the dashboard to manage the inventory of all equipment (i.e., hardware) and applications (i.e., software), and resources within the HCE - in all physical, virtual, colocation and cloud environments in the HCE. The Contractor shall:

1. Maintain a Configuration Management Database (CMDB) with the complete HCE hardware and software asset inventory including IaaS assets (e.g. virtual machines

and storage services) accessible through the dashboard and provide integration with and access to enterprise CMDB solution(s).

2. Record receipt of all incoming hardware and software items within an asset tracking and inventory management system and record changes in location for each item as they occur.
3. Provide retrieval, view, and download access to all asset information indicating location and status of each inventory item as well as maintenance and licensing agreements and expiration dates for all inventory items. Download access shall enable the export of data in processable formats (e.g., Microsoft EXCEL, PDF) for offline analysis.
4. Deliver a complete, fully validated inventory of all equipment, applications and system software within the HCE not less frequently than at four-month intervals in both the dashboard and as a separate analytical data file.

3.4 Change Management

The Contractor shall control change within the HCE in compliance with the enterprise change management process to ensure the completeness and integrity of all changes implemented within the HCE. The Contractor shall follow established DHS processes and procedures for adequate change management control and implementation.

The change processes shall manage the following components that may change in fulfillment of Task Orders:

- Hardware
- Architecture
- System software
- Application software
- Cloud IaaS services and resources

All documentation and procedures associated with the operation, support, and maintenance of systems, equipment, services, and applications shall be stored in the Information Repository.

3.5 Customer Satisfaction

The Contractor shall solicit an assessment of Customer satisfaction from each Task Order owner. Contractor shall design and implement surveys to capture and document customer satisfaction using Net Promoter Score to gauge Customer satisfaction. The Contractor shall develop and execute corrective action plans to remedy deficiencies identified through these surveys.

3.6 Quality Control

The Contractor shall develop and implement a Quality Management Program. The Contractor shall create and submit a Quality Management Plan (QMP) describing the standards, processes and procedures used to support the consistent delivery of high-quality, professional products and services provided in support of 24x7x365 HCE operation. The QMP shall be based on the Quality Assurance Surveillance Plan (QASP) provided by the +. The Contractor shall deliver the

initial QMP 60 days after Transition Task Order award and review and update the QMP at least annually.

The Contractor shall implement processes and procedures described in the QMP to meet and measure performance pursuant to the Government-provided SLAs. The Contractor shall not diminish the service offerings from the CSPs to a level lower than the published commercial cloud service, or standard SLAs (Acceptable Quality Levels [AQLs] in Section 12 correspond to SLAs), unless otherwise specified and approved by DHS.

3.6.1 Application Quality Control

The Contractor shall provide Application Quality Control services for applications hosted in the HCE in order to maintain application integrity. The Contractor shall manage Quality Control according to industry best practices and shall detect and report quality problems per contract SLAs and any SLAs particular to Task Orders.

3.6.2 Independent Verification and Validation Support

As directed by the COR, the Contractor shall provide cooperation and support to any Independent Verification and Validation (IV&V) project performed by or commissioned by DHS or the Department's designated representative.

3.7 Availability Management

The Contractor shall ensure CSPs provide a minimum availability of 99.9% for each service (e.g., virtual machine, object storage, virtual private cloud) incorporated into the HCE, unless otherwise published by the CSP. The Contractor shall ensure each service provided to DHS, meets or exceeds, the commercially advertised level or published SLA. The Contractor shall ensure that services launched by DHS in multiple cloud zones or regions continue to operate and remain available when any of the CSP's data centers are offline or unavailable. The Contractor shall ensure CSP services acquired for DHS have redundancy characteristics that ensure the capability for maintaining the minimum availability requirement.

3.8 Operations and Maintenance Services

The Contractor shall follow the industry recognized ITIL version 4 practices to provide lifecycle O&M support for the HCE. This includes installing and configuring hardware and system software on physical equipment, system software on cloud-based IaaS services, integrating, testing and securing physical and cloud resources, and conducting ongoing maintenance. The ongoing maintenance shall include asset management, change management, problem and incident management, continuity of operations, continuous monitoring, and decommissioning.

The Contractor shall apply a similar approach to providing lifecycle O&M support for customer applications in the HCE. The Contractor shall apply this lifecycle approach at the required classification levels: Unclassified, SBU, Secret, and Top Secret (TS), including Sensitive Compartmented Information (SCI).

The Contractor shall provide tiered service levels:

- Level 1 services apply to physical assets located in DC1 or in colocation centers - compute, storage, database, and networking devices.
- Level 2 services apply to all system software, including operating systems, database management systems, data backup systems and network software, in any HCE environment. System software also includes tools for managing and monitoring hardware and software components, problems and incidents, and resource management. Level 2 services may apply to physical assets within the HCE, virtual assets within the HCE, or to assets placed in HCE cloud environments.

3.8.1 Basic Level Service (Level 1)

Basic Level Service (Level 1) is a hosting service offered for physical assets installed within the HCE. Level 1 services include hardware installation and maintenance and network monitoring for equipment. This is the minimum level of service that is provided for all physical assets residing within the HCE. The Contractor shall ensure that equipment is installed in DC1 or in colocation facilities as appropriate and that the equipment is brought up to an operational state and the Contractor shall also provide the services described in this section. Basic Level Service provides network connectivity from the servers to the WAN point of demarcation for all systems hosted in the environment.

3.8.1.1 Installation

The Contractor shall perform all tasks necessary to properly install equipment to ensure all items are installed in the state as required by Task Orders. The Contractor shall test and document equipment and ensure that the enterprise change management process is followed. The Contractor shall ensure proper communication with the DHS COR, HCE service desk, DHS Data Center Operations Team, and facility management (whether NASA for DC1 installations or colocation facility management for colocation installations), as appropriate.

3.8.1.2 Hardware Maintenance

For all equipment within the HCE the Contractor shall:

1. Monitor equipment.
2. Ensure that maintenance agreements are renewed in a timely manner.
3. Activate maintenance agreements as and when service is scheduled or needed.
4. Record equipment identification, location, status and updates in the CMDB.
5. Document as-installed configurations.
6. Document as-installed network schematics.
7. Store all documentation in the Information Repository.

3.8.1.3 Configuration (Hardware/System)

The Contractor shall:

1. Configure the hardware systems based on DHS IT and Cybersecurity Policy, DHS Headquarters (HQ) standards, and as specified on Task Orders by the Ordering Component (if consistent with DHS HQ provided configuration guidelines).
2. Document and provide updates to the as-built documentation to the DHS Project Manager and store those updates in the Information Repository.
3. Maintain configuration information resulting from maintenance or change implementations in the HCE Information Repository and CMDB.

3.8.1.4 Incident and Problem Management

The Contractor shall:

1. Conduct automated monitoring of the operational status of each equipment item in the HCE and implement a data feed to the enterprise network operations center and to other enterprise systems, if required.
2. Provide real-time operational status of each equipment item of system component and respond if degradation occurs (e.g., providing integration with existing solutions and implementation of timely reporting and automation notification (s) to enterprise stakeholders for outages, as approved by DHS).

3.8.1.5 Decommissioning

The Contractor shall provide decommissioning services. The Contractor shall:

1. Retain images, settings, and data from the device to be decommissioned until there is written permission to delete/dispose of the data from the Task Order COR not to exceed 60 days.
2. Describe the provisioning, de-provisioning, and decommissioning status.
3. Track status changes in the Asset Inventory Tracking System in the dashboard.
4. Power down, de-rack, degauss, and sanitize decommissioned physical equipment and/or VMs in accordance with NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, DHS Information Security Policy, contract(s), and task order requirements.
5. Inventory, de-install, pack, and ship DHS Component GFE equipment, and prepare for pickup by either the customer for reuse or for disposal based on the customer's requirement.
6. Maintain and provide a clear chain of custody for all equipment movement and hard disk disposal.
7. Certify equipment throughout the operations of the system while hosted in the HCE in accordance with DHS Security Authorization (formerly Certification and Accreditation) policies and decommission appropriately.

3.8.2 Level 2 Support Services

Level 2 Managed Services are additional services offered for systems, software, and applications residing in the HCE. Level 2 services may be elected individually. For equipment resident in physical locations, individual Level 2 services represent additional services in addition to the basic Level 1 services. However, Level 2 services are not contingent upon ordering Level 1 services (i.e., in the case of services performed for cloud resources). Individual Level 2 services may be elected for systems, services, or applications implemented or managed in cloud

environments - whether on-premises private cloud or off-premises commercial cloud or Gov-Cloud environments provided by CSPs.

3.8.2.1 Operating System Installation, Configuration, & Management

The Contractor shall perform all the necessary functions to install, configure, maintain, and manage operating systems.

3.8.2.2 Software Patch and Release Management

The Contractor shall provide software patch and release management and application services to protect software from potential threats, maintain software operational functionality, comply with DHS Configuration Management Processes and Procedures, including, but not limited to, patch testing, installation, fixture, and deployment, and the support and implementation of DHS Data Center Service Resource Management Process. The Contractor shall comply with DHS Configuration Management Processes and Procedures in all HCE environments including cloud and colocation. The Contractor shall apply operating system, application, solution and security patches as received from software vendors and approved by DHS and shall support and manage processes for waivers, exceptions, and Plans of Action and Milestones (POA&Ms) in a timely manner.

3.8.2.3 Storage Management

The Contractor shall provide storage services and utility offerings for managing customer-owned data storage assets residing in HCE physical locations and cloud-based storage assets or services. The Contractor shall ensure that DHS data is not backed up, stored, replicated, or transmitted in any manner outside of the physical boundaries of the Continental United States. The Contractor shall also ensure that only U.S. citizens provide support services for resources acquired for DHS, as required by risk-based and security authorization decisions.

The Contractor shall ensure the operations of each application, storage device, or service as required on Task Orders.

The Contractor shall:

1. Install and configure physical storage devices to include SAN, network attached storage (NAS), and tape libraries.
2. Configure cloud storage resources including any management software and manage the allocation and retraction of storage in a dedicated and/or virtualized storage environment.
3. Monitor and manage storage capacity to keep utilization below the ceiling specified in Section 12.
4. Use automated tools to perform data compaction, compression, and migration tasks.

3.8.2.4 Backup and Restore

The Contractor shall perform backup, archival, and restoration services to include incremental backups daily and full backups weekly and manage backup scripts to backup critical operating system and system data files including all system batch processes, as required by the respective system. Backup and restoration may be elected for systems, applications, and data stores residing

in any HCE environment. The Contractor shall restore operating systems according to the owning Component's Disaster Recovery (DR) plan and specific system recovery objectives.

The Contractor shall manage physical backup media (e.g., magnetic tape), adhere to or define media vaulting policies, and ensure offsite vaulting and storage. The Contractor shall ensure the transfer of physical backup media to and from offsite storage facilities as required by task orders and in support of recovery efforts. The Contractor shall provide the offsite storage service within the contract CLIN structure.

3.8.2.5 Database Support

The Contractor shall provide database support, including installation, configuration, management, backup, and security.

The Contractor shall provide options to synchronize, replicate, backup and restore data from any environment within the HCE to another (e.g., from DC1 to a CSP).

4 Professional Services

The Contractor shall provide professional lifecycle support services for customer systems and applications including custom components, commercial off the shelf (COTS) products, and associated data sources (e.g., databases and data storage) within the HCE.

Professional services include but are not limited to the following:

- System assurance
- Initial Application Baselining
- Application and System Installation and Testing
- Application and Systems Monitoring, Maintenance and Enhancement
- Application and System Migration, Modernization, and Rationalization within the HCE
- Integration, Testing, and Deployment
- Application and System Security
- Application and System Decommissioning
- End User Training
- Application and System Service Desk
- Disaster Recovery Services
- Evolving Technology Incorporation
- Operating Systems and Data Management Services not included in Level 2
- Systems and Network Engineering

Professional services do not include development of new applications or the addition of significant functionality to existing applications.

5 Contractor Personnel

5.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this PWS.

5.2 Key Personnel Positions

The Contractor shall propose a staffing plan that identifies Key personnel. Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer. The minimum key personnel required by the Government are:

- Program Manager (PM)
- Service Delivery Manager (SDM)
- Security Manager

The Contractor may propose any additional Key personnel deemed necessary for management of the contract.

Additional Key Personnel may be proposed and incorporated into individual Task Orders. If the Government determines that certain personnel are “key” to successful completion of a Task Order, they will be designated as "Key Task Order Personnel" in the Task Order.

Key Personnel

Key Personnel Position	Required Education	Required Clearance & Certifications	Key Personnel Experience	Position Description
Program Manager (PM)	Master's degree or higher in Computer Science, Business Administration Science, Mathematics or Engineering	Clearance: Top Secret Certification: PMP ITIL 4 Managing Professional	15+ Years of IT Experience, 10 of which are in building, operating, and improving environments similar to the DHS HCE.	As lead executive, the PM has overall responsibility for all financial, technical, administrative, contractual, and personnel aspects of the HCE Support Indefinite Delivery Indefinite Quantity (IDIQ) Contract and all Component Task Orders. The PM is also the key interface with DHS executives. Manages, directs, and allocates resources to support the HCE program; supported by Contractor corporate executives to make sure that the HCE provides on-time delivery of top-quality services to DHS.
Service Delivery Manager (SDM)	Bachelor's degree or higher in Computer Science, Business Administration Science, Mathematics or Engineering	Clearance: Top Secret Certification: ITIL 4 Managing Professional	10+ Years of IT Experience, 8 of which are in building, operating, and improving environments similar to the DHS HCE.	The Service Delivery Manager (SDM) oversees all aspects of the delivery of services and service technology across the HCE Enterprise including coordination of requirements across all Task Orders. The SDM establishes policies designed to ensure consistently high service performance, monitors employees and evaluates customer feedback to develop quality improvement processes.
Security Manager (SM)	Bachelor's degree or higher in Computer Science, Business Administration Science, Mathematics or Engineering	Clearance: Top Secret Certification: CISSP and CCSP or, CISSP and GIAC GCSA or, CISM and CCSP or, CISM and GIAC GCSA	10+ Years of IT Experience, 8 of which are in Cybersecurity Management.	The Security Manager (SM) shall act as the Contractor's Corporate Cybersecurity Officer. The SM shall interface with COR who will interface with other DHS officials on all cybersecurity matters, to include physical, personnel, and protection of all sensitive documents/material handled by the Contractor. The SM ensures Contractor compliance with all security requirements under this contract and is responsible for determining enterprise information security standards across the HCE and for the development, implementation, and execution of IT Security Policies, Standards and Procedures.

5.2.1 Program Manager

The Contractor shall provide a Program Manager who shall be responsible for all Contractor work performed under this Performance Work Statement. The Program Manager shall be a single point of contact for the Contracting Officer and the COR. The name of the Program Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Program Manager, shall be provided to the Government as part of the Contractor's proposal. The Program Manager is further designated as *Key* by the Government. During any absence of the Program Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under the contract. The Program Manager and all designated alternates shall be able to read, write, speak, and understand English. Additionally, the Contractor shall not replace the Program Manager without prior approval from the Contracting Officer.

5.2.1.1 Program Manager Availability

The Program Manager shall be available to the COR via telephone between the hours of 8:00 AM and 5:00 PM Eastern Time Monday through Friday and available for escalation on a 24x7x365 basis and shall respond to requests for discussion or resolution of technical problems within 2 hours of notification in accordance with the established escalation processes located in the Program Plan.

5.3 Employee Identification

5.3.1 Employees Visiting Government Sites

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

5.3.2 Employees Working at Government Sites

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display Government-issued badges in plain view above the waist at all times.

5.4 Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or

the Department of Homeland Security. The Program Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

5.5 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer or the COR acting for the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

5.5.1 Personnel

5.5.1.1 Employment Eligibility

The Contractor shall ensure that each employee and potential employee provides his/her name and social security number (not card) so that the Government may verify the validity of the number. If the number is not valid, that employee will not be allowed to work on the contract until the problem is resolved. The Contractor shall be responsible to the Government for acts and omissions of their employees as well as Sub-contractor(s) and their employees.

Subject to existing law, regulations, and/or other provisions of this contract, illegal or undocumented aliens shall not be employed by the Contractor or perform on this contract. The Contractor shall ensure this provision is expressly incorporated into any and all sub-contracts or subordinate agreements issued in support of this contract.

5.5.1.2 Continued Eligibility

If a prospective employee is found to be ineligible for access to DHS facilities or information, the COR will advise the Contractor that the employee shall not continue to work or be assigned to work under the contract.

DHS reserves the right to deny and/or restrict entrance to Government facilities, prohibit employees from assigned work under the contract, or deny and/or restrict handling of classified documents/material to any Contractor employee who DHS determines to present a risk of compromising sensitive Government information.

The Contractor shall report to the appropriate Government Security Office (r) and to the COR any and all adverse information brought to their attention concerning employees performing under this contract. Reports based on rumor or innuendo shall not be included. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employee's name and social security number, along with the adverse information being reported.

5.5.1.3 Termination

During the period of this IDIQ, the rights of ingress and egress to and from any office for Contractor's personnel shall be made available, as deemed necessary by the Government. All Contractor employees, whose duties under this contract require their presence at any

Government facility, shall be clearly identifiable by a distinctive badge furnished by the Government. In addition, corporate identification badges shall be worn on the outer garment at all times. Obtaining the corporate identification badge is the sole responsibility of the Contractor.

All prescribed information shall immediately be delivered to the appropriate Government Security Office (r) for cancellation or disposition upon the termination of employment of any Contractor personnel. All on-site Contractor personnel shall abide by security regulations applicable to that site.

The Contractor shall return to the COR all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

5.5.1.4 Suitability Determination

DHS shall exercise full control over granting, denying, withholding or terminating unescorted government facility and/or access to or handling of both classified and sensitive Government information to Contractor employees based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by Office of Security and Integrity (OSI).

5.5.1.5 Information Technology Security Clearance

When sensitive Government information is processed on DHS telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed and adhere to the procedures governing such data as outlined in “DHS IT Security Program - Publication DHS MD 4300.Pub”. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with DHS security policy are subject to having their access to DHS IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

5.5.1.6 Information Technology Security Training and Oversight

All Contractor employees using DHS automated systems or processing DHS sensitive data shall be required to receive Security Awareness Training.

Contractors involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of OCIO, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. DHS Contractors with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access OCIO information systems will be continually evaluated while performing these duties. Supervisors shall be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures shall be reported to the Network Operations Center, Information Security Official, or OSI.

5.5.2 Personnel Security Services

The Contractor shall perform the following work activities to provide personnel security services. Any customer-specific security requirements will be specified in Task Orders.

1. Abide by the Contract Security Classification Specification (DD-254), to be included in the contract, the National Industrial Security Program Operating Manual (NISPOM), and any agency-specific requirements to protect DHS classified information.
2. Appoint a security officer to interface with the DHS Security Office on all matters pertaining to security including physical, personnel, and protection of classified material.
3. Make all procedures, methods, and facilities available to the Contracting Officer's Representative (COR) and DHS Security Office for inspection and take appropriate action to rectify any noncompliance.
4. Facilitate the completion and submission of forms required to obtain clearances.
5. Ensure that only personnel with appropriate clearances are permitted access to sensitive data and clearances are commensurate with the security level of the data.
6. Ensure that all Contractor personnel receive security awareness training at least annually and that they understand and sign the rules of behavior for all systems that they access.
7. Appoint a Contractor's Industrial Security Office (ISO) who shall support the DHS HCE by performing the following activities:
    a. Make sure that Contractor personnel assigned directly to this effort are U.S. citizens.
    b. Provide DHS with a Contractor Personnel Summary List (CPSL) that presents information about the current clearances of the Contractor's proposed personnel including their full names, Social Security numbers, clearances held, name of granting Agency, date on which clearances were granted, dates of background investigation (BI), and polygraphs performed in compliance with proposal requirements.
8. The Contractor has instituted a thorough security awareness and prescreening program for candidates being considered for DHS-trusted access approval, which shall be employed for the DHS HCE.

a. Candidates being considered for this program shall have undergone an initial Contractor-sponsored background investigation, drug-screening test, and a tiered interview process.
b. Candidates shall participate in a second-level security screening process that is conducted by the ISO and is relevant to the Contractor Industrial Security Program process. The screening includes a thorough review of the candidate's Questionnaire for National Security Positions (Standard Form [SF]-86), and an in-depth security interview during which the criteria for meeting Intelligence Community Directive (ICD) 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, and Other Controlled Access Program Information, standards is explained and an assessment is made of the candidate's suitability for a position of trust. Results of the interview assist the ISO in predicting the candidate's probability of successfully completing the DHS' industrial security process, after which the ISO makes a recommendation to the program manager concerning the advisability of the candidate's continuing with the process.
c. The Contractor shall make sure that access to SCI is granted on a program-by-program basis as a result of inclusion on a specific program's roster and a verified Need-to-Know. When it is determined that access to SCI is required, the program or proposal manager shall submit to the Contractor Security Officer (CSO) the names of employees requiring access on the project, after gaining approval from the appropriate COR. After an interview with the potential nominee, in which the CSO determines the employee's suitability and understanding of the obligations of TS/SCI-level clearance, the CSO shall submit these names to the appropriate DHS technical element for nomination.

9. Security Approval Process:
   a. The Contractor shall make sure that when a qualified candidate has been selected, the ISO submits the required documentation to the DHS HQ's Industrial Security Office and requests the appropriate level of access. During the approval process, the ISO remains in close contact with the Government security representative to coordinate scheduling of polygraph interviews, personal interviews, and required briefings.
   b. The Contractor shall make sure that upon notification from the Industrial Security Office, the employee shall be indoctrinated as appropriate and the CSO shall amend the project access list to include the employee's name. The Contractor shall not authorize an employee to have access to DHS SCI until the Contractor has received an approval on Form 4311. When the program or proposal manager advises the CSO that the employee no longer requires access to the project, the CSO notifies and debriefs the employee.
10. Briefing, Re-briefing, Debriefing, Education - The Contractor shall make sure that all initial Industrial Security Staff Approval (ISSA)/TS indoctrination and briefings of Contractor personnel shall be performed or controlled at the program's agency. The Contractor shall conduct initial security briefings at the ISSA/TS and ISSA/S levels. A

mandatory annual awareness briefing is given to all Contractor employees who hold a security clearance. Security training is offered, and relevant periodic memos are distributed to maintain the Contractor personnel's security awareness.

11. Reinvestigating - The Contractor shall make sure that security background reinvestigation requests are submitted to the DHS every four and one-half years. Requisite forms, including Form 4311 and an updated SF-86, are submitted to initiate the BI. When applicable, employees undergo polygraphs during this process, if requested to do so. The ISO monitors this procedure, and all documentation is maintained within the ISO. When special DHS reinvestigations are required, they are also coordinated by the ISO.
12. Security Violation Program - The Contractor shall comply with all DCIDs with regard to security incidents. The ISO initiates an inquiry immediately upon notification that an incident or possible incident has taken place. The ISO promptly notifies DHS Security and Program Managers by means of a preliminary report and follows up with a final report. Of paramount importance is a guarantee, as soon as possible, that an incident has been contained. Just as importantly, measures to prevent a recurrence are planned and implemented after consulting with the DHS Security Officer responsible for the contract. For serious, repeated, or negligent security infractions, Contractor employees are subject to an escalating series of penalties that includes termination.
13. Control of Cleaning Force and Maintenance Program - The Contractor shall make sure that all cleaning personnel requiring access to DHS spaces in the building either have the appropriate clearance for those spaces or are escorted by appropriately cleared Contractor personnel at all times.

5.5.3 SBU, Secret, Top Secret and SCI Processing Facilities.

5.5.3.1 Sensitive But Unclassified (SBU) Systems Requirements

OCIO has determined that performance of this contract requires the Contractor access to sensitive but unclassified (SBU) information. SBU is unclassified information for official use only. Contractor employees that do not have a security clearance and require access to SBU information will be given a suitability determination.

Data Security - SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design and ensure that they meet the minimum requirements as set forth in the DHS IT and cybersecurity policies and procedures. These requirements include:

Integrity - The computer systems used for processing SBU data shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.

Confidentiality - Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability

assessment shall be performed to determine if threats to the SBU information or data exist. If it exists, data encryption shall be used to mitigate such threats.

Availability - Controls shall be included to ensure that the system is continuously working and that all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.

Data Labeling - The Contractor shall ensure that documents and media are labeled consistent with the DHS Sensitive Systems Policy for systems and services delivered and operated by the Contractor.

5.5.3.2 Secret Systems Requirements

The Contractor shall provide infrastructure and support for applications, systems, and services classified at the Secret level.

5.5.3.3 Top Secret Systems Requirements

The Contractor shall provide infrastructure and support for applications, systems, and services classified at the Top-Secret level.

5.5.3.4 TS/SCI SCIF Requirements

The Contractor shall cooperate and comply with Government regulations to maintain the security posture of DC1 Sensitive Compartmented Information Facilities (SCIF) to meet the Department's TS and SCI requirements. The Contractor shall support DHS efforts to maintain SCI accreditation as required. This task includes but is not limited to the following:

1. Coordination with the facilities provider
2. Support in compliance with DHS and Government Security Directives

6 Other Applicable Conditions

6.1 Security

Contractor access to classified information is required under this PWS. The maximum level of classification is Top Secret/SCI. The Contractor shall be required to hold a Top Secret Facility Clearance. The details will be specified in a Department of Defense (DD) Form 254.

6.2 Hours of Operation

Contractor shall operate HCE on a 24x7x365 basis.

6.3 Program Plan

The Contractor shall provide a draft Program Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Program Plan to the COR not later than 90 business days after the Post Award Conference. Updates to the Program Plan and sub-components are required at a minimum, annually. The Program Plan shall address how the Contractor will manage the HCE, communicate with DHS management and customers, staff the

effort, select samples of customers for survey purposes, and escalate technical problems and issues to ensure resolution.

The Program Plan at a minimum shall document the vendors approach to communications, staffing, security, infrastructure design, LAN design and support, LAN and server support, HCE and network architecture design, disaster recovery, random sampling method, severity classification, application support matrix, and HCE Concept of Operations (CONOPs).

6.4 Operational Plans and Reports

6.4.1 Business Continuity Plan

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 60 business days after the date of Transition Task Order award and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- How the Contractor will communicate with the Government during emergencies
- A list of primary and alternate Contractor points of contact, for each primary and alternate:
    - Telephone numbers
    - Email addresses

The BCP shall be activated immediately after determining that an emergency has occurred, shall be operational within 12 elapsed hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life-threatening emergency, the COR shall immediately contact the Contractor Program Manager to ascertain the status of any Contractor personnel who were in Government controlled space affected by the emergency. When any disruption of normal, daily operations occurs, the Contractor Program Manager and the COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and Contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g., email, webmail, telephone, FAX, courier, etc.)
- Essential Contractor work products expected to be continued, by priority

The Government and Contractor Program Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within

the scope of their contract shall charge those hours accurately in accordance with the terms of the contract.

6.4.2 Contingency Plans

The Contractor shall develop and maintain Contingency Plans (CPs) for all GSS systems with the requirements for the FIPS 199 Categorization. The Contactor shall test CPs annually by the anniversary date of the Authority to Operate (ATO) and results shall be uploaded into Security Authorization (SA) repository (e.g., Xacta), as required.

6.4.3 Patch Management Plan

The contractor shall develop a Patch Management Plan that describes the agreed to Security Patch Management support along with a high-level model describing the end-to-end process from vendor alert notification through DHS environment applicability assessment, to testing and implementation.

6.4.4 Anti-Virus Management Report

The Contractor shall generate a report on the anti-virus implementation and version status of all managed and monitored computing systems in the HCE.

6.4.5 General Support System (GSS) for Compliance with OMB A-130 - System Security Plan/Security Plan

The Contractor shall develop and maintain System Security Plans (SSP) and/or Security Plan for each GSS supporting the management and operation of the HCE in compliance with Office of Management and Budget (OMB) Circular No. A- 130, Management of Federal Information Resources, November 30, 2000, Appendix III (Security), and DHS Information Security Policy.

6.4.6 Security Plan (SP) - Compliance with FIPS 199

The Contractor shall develop a Security Plan (SP) that is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SP shall be based upon the completion of the DHS FIPS 199 workbook to categorize a system or application. The SP shall be completed as part of the System or Release Definition Process in the DHS Systems Engineering Life Cycle and shall not be waived or tailored.

6.4.7 Government Furnished Equipment Report

Contractor shall provide a detailed and updated accounting of all Government Furnished Equipment (GFE) not already included in the CMDB and issued to the Contractor to enable fulfillment of responsibilities under this contract, including equipment, software, and data in the Contractor's custody.

6.5 Recurring Reports

The Contractor’s Program Manager shall provide regular reporting to the Government on a recurring basis.

6.5.1 Progress Reports

The Program Manager shall provide a monthly Program Report and a monthly Financial Report to the Contracting Officer and COR via electronic mail. These reports shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category for time and material and labor hour tasks, all direct costs by line item at the individual service or resource level, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period. The Progress and Financial reports shall be delivered as two separate documents.

6.5.1.1 Monthly Financial Report

The Monthly Financial report shall provide the program financial status including the status of the overall Program and each Task Order. The report shall include all the information needed to describe financial status of each Task Order as well as a summary of invoices across all Task Orders. Information should include but not be limited to actual vs. planned costs, purchases by Contract Line Item Number (CLIN) and Category, obligations by Component and Task Order, expenses, trends, and OMB Circular No. A-11 data elements. The Monthly Financial report shall also include a report of catalog purchases detailing the specific items purchased under the Catalog CLINs, the cost of each purchase, and a reference to the published price schedule for each purchased item. The report shall be delivered monthly through dashboard update with data available for Government review and download in a processable format.

6.5.1.2 Monthly Program Report (MPR)

The Monthly Program Report shall accompany the Monthly Financial report. The MPR shall provide status information for DHS operations and program, technical, and other types of activities for the previous month. As required, the MPR shall include but not be limited to the following:

- Incident management and associated trends
- Problem management and associated trends
- Configuration Report
- Asset Management Reports
- Service Management Reports
- SLA Performance Reports
- Task Order Proposal and ROM Status Reports
- Planning and Engineering (P&E) Progress Reports
- Hardware Inventory Data
- Service Inventory Data
- Colocation Services Data
- Lost/Damaged equipment
- Software Licenses Inventory including application or system owner, software type, description, type of license (e.g., enterprise, single site), version, cost, date of acquisition, date of installation, and anticipated end of software assurance date
- Change Management Monthly Statistical Reports
- Statistical Availability Management Monthly Reports

- Inventory Validation Status Reports
- Recommendations for the incorporation of new or emerging technologies within the HCE - hardware, software applications, or CSP service offerings.

This information shall be continuously available in dashboards on an as needed basis. However, the necessary information shall be formally delivered to the CO and COR on a monthly basis.

6.5.1.3 Contractor Personnel Summary

The Contractor shall provide a monthly staffing report identifying all Contractor personnel having been granted Entry on Duty (EOD).

6.5.2 Quarterly Capacity Management Report

The Contractor shall provide a Capacity Management Report to the Government IDIQ COR quarterly. The report shall display information (network components, fiber and Ethernet capacity/availability, routers, switches, IDS, Firewall, etc.) on current state as well as 12-month forecast of capacity on Level 1 and Level 2 systems by Component for current quarter trended by month.

6.5.3 Service Level Agreement Level of Service Report

The Contractor shall generate a monthly Level of Service report that includes the level of service delivered compared to the requirements in each SLA monthly for the previous calendar month including an SLA incentive/disincentive evaluation report. The report shall also describe trends in service delivery including a comparison to the previous month, previous year, and same month during the previous year.

6.5.4 Service Quality Report

The Contractor shall generate a monthly Service Quality Report that addresses the forward-view of service delivery, new business requirements or new business activities that have a dependency on or impact to system availability, and a historical view of operations and past system availability trends. The report shall include a comparison of service levels delivered compared to the requirements in each SLA by month for the previous calendar month including an SLA incentive/disincentive evaluation report. The report shall also describe trends in service delivery including a comparison to the previous month, previous year, and same month during the previous year.

6.6 General Report Requirements

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (e.g., Windows 10 and Microsoft Office Applications, PDF). Written reports shall be uploaded to the Information Repository and be available through Dashboard access.

6.7 Meetings - Formal and Informal

Contractor shall provide agendas, take attendance, and record and distribute minutes of all formal meetings and informal informational meetings as appropriate.

6.7.1 Post Award Conference

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 14 business days after the date of contract award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft Program Plan. The Post Award Conference will be held at the Government's facility, located at an address to be specified at the time of contract award or via teleconference. Post Award briefing slides shall be provided to the COR, 2 business days prior to conference. The briefing slides shall be updated and delivered 5 days after Post Award Conference.

6.7.2 Weekly Progress Meetings

The Contractor's Program Manager and appropriate staff shall meet with the COR weekly and upon request to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place via teleconference.

6.7.3 Monthly Progress Meetings

The Contractor's Program Manager and appropriate staff shall meet with the COR monthly to conduct a formal status review meeting. These meetings shall take place via teleconference. The Progress meeting should review critical items in the Monthly Financial Report and the Monthly Progress Report.

6.7.4 Service Quality Review (SQR)

The Contractor shall host quarterly Service Quality Review (SQR) meetings. The Contractor shall lead the agenda and discussion. Part of the agenda will be dedicated to the forward-view, new business requirements or new business activities that have a dependency on or impact to system availability. Part of the agenda will be dedicated to a historical view and past system and service availability trends.

6.8 Pricing Catalogs

Note: Any reference made to a specific brand name in the Attachment J-1, Pricing Schedule is solely for estimating and evaluation purposes ONLY, and will not be incorporated at time of the IDIQ Contract Award.

The Contractor shall manage a catalog that provides DHS access to published price lists for COTS Equipment and Software, Infrastructure as a Service (IaaS) and Professional Service offerings that are not specifically named and priced in Attachment J-1, Pricing Schedule. The catalog allows DHS to purchase additional offerings that are within scope of the DCCO IDIQ contract and necessary in order to manage the Hybrid Computing Environment (HCE) as

described in this Performance Work Statement. The catalog shall be comprised of the following: e-location links to the products and services, item number; item description; the published price for each item; the minimum discount per catalog category; and any additional discounts offered by the Contractor for that specific product or service. The catalog shall be broken down into three categories: COTS equipment and software; Professional Services; and IaaS.

- The COTS Equipment and Software catalog(s) shall link to published price lists that contain Compute, Storage and Network equipment and software. The catalog shall list all the equipment necessary including security appliances and associated maintenance agreements to operate and maintain the HCE. Any software purchased must run on equipment within the HCE or directly support systems within the HCE.
- The Cloud (IaaS) catalog(s) shall link to the compute, storage, network, database, and ancillary resources from the Cloud Service Providers.
- The Professional Services catalog shall link to all the labor categories associated with the HCE in support of Section 4 of the Performance Work Statement (PWS).

The Contractor shall maintain a history of all DCCO catalog purchases and provide a dashboard of all historical catalog purchases available for review and download and include a summary in the Monthly Financial report.

The Contractor shall provide a catalog user guide to instruct the user on the access, use, and functionality of the catalog.

The catalogs are not a mandatory source of supply. The Government may use other mechanisms to acquire these products and services. All requests to purchase a product and/or service via a Catalog CLIN must be approved by the IDIQ COR.

6.9 Protection of Information

Contractor access to information protected under the Privacy Act is required under this PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

Contractor access to proprietary information is required under this PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

6.10 Section 508 Compliance

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with

disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

    Item that contains Information and Communications Technology (ICT): Security Equipment

        Applicable Exception: N/A Authorization #: N/A

        Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

        Applicable 508 requirements for electronic content features and components (including Internet and Intranet website; Electronic reports): Does not apply

        Applicable 508 requirements for software features and components (including Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

        Applicable 508 requirements for hardware features and components (including Servers): All requirements in Chapter 4 apply

        Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

    Item that contains Information and Communications Technology (ICT): Networking equipment

        Applicable Exception: N/A Authorization #: N/A

        Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater

accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components: Does not apply

Applicable 508 requirements for software features and components (including Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including Servers): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Hosting equipment

Applicable Exception: N/A Authorization #: N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components: Does not apply

Applicable 508 requirements for software features and components (including Software infrastructure): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components (including Servers): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Virtualized Software

Applicable Exception: N/A Authorization #: N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components (including Internet and Intranet website; Electronic documents; Electronic forms; Electronic document templates; Electronic emergency notifications; Electronic surveys; Electronic reports; Electronic training materials; Multi-media (video/audio)): Does not apply

Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications; Electronic content and software authoring tools and platforms; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

Applicable 508 requirements for hardware features and components (including Servers): All requirements in Chapter 4 apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Software as a Service

Applicable Exception: N/A Authorization #: N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components (including Electronic documents; Electronic forms; Electronic document templates; Electronic surveys; Electronic reports): Does not apply

Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications; Electronic content and software authoring tools and platforms; Software infrastructure; Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application, 504 Authoring Tools

Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Email Services

Applicable Exception: N/A Authorization #: N/A

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components (including Internet and Intranet website): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

Applicable 508 requirements for software features and components (including Service Offerings): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

Applicable 508 requirements for hardware features and components: Does not apply

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

2. When providing and managing hosting services for ICT, the Contractor shall ensure the hosting service does not reduce the item's original level of Section 508 conformance before providing the hosting service.

3. When providing installation, configuration or integration services for ICT, the Contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

4. When providing maintenance upgrades, substitutions, and replacements to ICT, the Contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed substitutions and replacements prior to acceptance. The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be located at https://www.itic.org/policy/accessibility/vpat.

5. When developing or modifying ICT for the government, the Contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.

6. When developing or modifying web and software ICT, the Contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the DHS Trusted Tester Methodology currently approved for use, as defined at https://www.dhs.gov/508-testing. The Contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g. "DHS Certified Trusted Testers") to conduct accessibility testing. Information on how testers can become certified is located at https://www.dhs.gov/trusted-tester.

7. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents - Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/508-testing.

8. When developing or modifying software that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the Contractor shall ensure software can be used to create electronic content that conforms to the Section 508 standards.

9. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

10. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018.

Instructions to Offerors

1. For each commercially available Information and Communications Technology (ICT) item offered through this contract, the Offeror shall provide an Accessibility Conformance Report (ACR). The ACR shall be created using the Voluntary Product Accessibility Template Version 2.0 508 (or later). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed in accordance with all the instructions provided in the VPAT template. Each ACR must address the applicable Section 508 requirements referenced in the Work Statement. Each ACR shall state exactly how the ICT meets the applicable standards in the "remarks/explanations" column, or through additional narrative. All "Supports", "Supports with Exceptions", "Does Not Support", and "Not Applicable" (N/A) responses must be explained in the remarks/explanations column or through additional narrative. The offeror is cautioned to address each standard individually and with specificity, and to be clear whether conformance is achieved throughout the entire ICT Item (for example - user functionality, administrator functionality, and reporting), or only in limited areas of the ICT Item. The ACR shall provide a description of the evaluation methods used to support Section 508 conformance claims. The agency reserves the right, prior to making an award decision, to perform testing on some or all of the Offeror's proposed ICT items to validate Section 508 conformance claims made in the ACR.

2. For each ICT Item that will be developed, modified, installed, configured, integrated, maintained, or hosted by the Contractor pursuant to this contract, the offeror shall provide an acknowledgement of the Section 508 requirements and a detailed explanation of the Offerors plan to ensure conformance with the requirements. The Offeror shall also describe the evaluation methods that will be used to validate for conformance to the Section 508 Standards.

3. For each commercially available authoring tool offered that generates electronic content (e.g., an authoring tool that is used to create html pages, reports, surveys, charts, dashboards, etc.), the Offeror shall describe the level of Section 508 compliance supported for the content that can be generated.

4. The offeror shall describe plans for features that do not fully conform to the Section 508 Standards.

Acceptance Criteria

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the Contractor to provide the following:

    - Accessibility test results based on the required test methods.
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation of core functions that cannot be accessed by persons with disabilities.

- Documentation on how to configure and install the ICT Item to support accessibility.
- Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content - where applicable).

2. Before accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represent a higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

6.11 Security Assurances

DHS Management Directive 4300 requires compliance with standards set forth by NIST for evaluating computer systems used for processing Sensitive But Unclassified (SBU) information. The Contractor shall:

1. Ensure that requirements allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements for systems and services delivered and operated by the Contractor.
2. Ensure that systems offer the following visible security features:

6.11.1 User Identification and Authentication (I&A)

I&A is the process of telling a system the identity of a subject (for example, a user) (Identification) and providing that the subject is who it claims to be (Authentication). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall use strong (two factor) authentication that conforms to established DHS standards. All DHS Identification and Authentication shall be done using AppAuth or its successor and in accordance with HSPD-12 requirements. Under no circumstances will Identification and Authentication be performed by other than the OCIO standard system in use at the time of a systems development.

6.11.2 Discretionary Access Control (DAC)

DAC is a DHS access policy that restricts access to system objects (e.g., files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.

6.11.3 Object Reuse

Object Reuse is the reassignment to a subject (e.g., user) of a medium that previously contained an object (e.g., file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation**.**

6.11.4 Clauses

The following DHS clauses will be incorporated into the IDIQ contract and resulting Task Orders.

1) Information Technology Security and Privacy Training (MAR 2015)
2) Safeguarding of Sensitive Information (March 2015)
3) 3052.204-70 Security requirements for unclassified information technology resources.
4) 3052.204-71 (Alt 1) Contractor employee access.

6.11.4.1 Information Technology Security and Privacy Training (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall

maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually. The COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

6.11.4.2 Safeguarding of Sensitive Information (MAR 2015)

a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions*. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique

identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's

license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO

expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the

Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

6.11.5 Banner Pages

The Contractor shall ensure that DHS systems provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages but shall apply to intranet applications.

6.11.6 DHS HLS EA Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this PWS and associated Task Orders. Specifically, the Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

All developed solutions and requirements shall be compliant with the HLS EA.

All IT hardware or software shall be compliant with the HLS EA.

Technology Reference Model (TRM) Standards and Products Profile.

All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS.

Enterprise Data Management Office (EDMO) for review and Insertion into the DHS Data Reference Model.

7 Government Terms & Definitions

Component. For the purposes of this PWS, "Component" means any DHS entity requesting any of the IT infrastructure services or support described herein.

Components include DHS Operating Components:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Emergency Management Agency (FEMA)
- Federal Law Enforcement Training Centers (FLETC)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard (USCG)
- U.S. Customs and Border Protection (CBP)

- U.S. Immigration and Customs Enforcement (ICE)
- U.S. Secret Service (USSS)

Components also include various Headquarters offices and directorates including but not limited to:

- Countering Weapons of Mass Destruction Office (CWMD)
- Management Directorate (MGMT)
- Office of Intelligence and Analysis (I&A)
- Office of the Chief Financial Officer (OCFO)
- Office of the Chief Information Officer (OCIO)
- Office of the Chief Information Security Officer (OCISO)
- Office of the Chief Procurement Officer (OCPO)
- Office of the Inspector General (OIG)
- Science and Technology Directorate (S&T)

Contracting Officer's Representative (COR). The DHS federal employee who provides day to day direction to the Contractor and who serves as the voice of the Contracting Officer. The COR is the official recipient for all Contractor deliverables and conducts quality reviews of all deliverables.

8 Government Furnished Resources

The Government will provide the workspace necessary to perform the on-site portion of Contractor services required in this contract, unless specifically stated otherwise in this work statement. Equipment and supplies may be supplied if approved by the Government.

The Government will provide the equipment and software necessary to support the GSS described in Section 1.1. The details of the included hardware and software will be provided in the Reading Room after Phase 1 of the proposal evaluation process.

The Contractor shall use Government furnished facilities and property initially for the performance of work under this contract and shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear. Equipment and supplies may be provided on a case by case basis when approved by the Government.

The Government will provide copies of the references cited in PWS 1.4 and Appendix A at the Post Award Conference.

The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

9 Contractor Furnished Equipment

The Contractor shall furnish all materials, equipment, and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in PWS 8.0.

At the Contractor's discretion any computing and communications infrastructure provided to host Contractor furnished software and systems may consist of appropriately approved physical servers, physical networking components, and data storage devices to be installed within one or more HCE physical locations. Infrastructure may also consist of virtual resources within commercial or private cloud environments or any hybrid of physical and virtual resources.

All contractor furnished equipment (e.g., laptops, hardware) to be used on, or connected to, DHS networks or infrastructure shall be approved by DHS adhering to DHS IT and Cybersecurity policy and procedures (e.g., imaging laptops).

10 Government Acceptance Period

The COR will review deliverables prior to acceptance and provide the Contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

10.1 COR Review Timeframe

The COR will have 10 business days to review deliverables and make comments. The Contractor shall have 7 business days to make corrections and redeliver.

10.2 Other Review Times

All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Program Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

11 Deliverables

All document deliverables shall be provided in electronic format. Unless indicated otherwise, the Contractor shall provide all deliverables in Microsoft Office format to the COR via email in addition to loading those deliverables to the Information Repository. Data deliverables shall be posted to dashboards with separate notice to the COR of completion of each deliverable and posting. The Contractor shall maintain an electronic copy of each document deliverable on the OCIO/DCD document repository.

The Government will provide clarification on requirements, templates, standards, and guidelines on all deliverables when clarification is not provided in the Task Order. All document tables of contents will be agreed to jointly with the Government prior to any action taken by the Contractor.

Contract level deliverables are listed in the following table. Additional deliverables may be specified at the Task Order level.

PWS Section	Deliverable	Description	Due	Delivered To
6.7.1	Post Award Conference Briefing Slides	Slide presented during Post Award Conference. Briefing deck shall discuss the technical and contracting objectives of this contract	2 days prior to Post Award Conference (6.7.1). Updates due 5 days after Post Award Conference.	IDIQ COR
6.3	Program Plan	The Program Plan shall address how the Contractor will manage and operate the HCE.	Draft at Post Award Meeting; Final 90 days after the Post Award meeting; Updates annually or within 30 days of major changes.	IDIQ COR
2.1.14.1	Transition-In: Onsite Assessment	Assessment of the state of data center and HCE operations and baseline processes and procedures at Transition-In.	15 days after Transition- in Task Order award.	IDIQ COR
2.1.14.1	Transition-In Plan	Plan for assuming control of management and operation of data center and HCE overall operations.	Draft 30 days after Transition-In Task Order award; Final 90 days after Transition Task Order award.	IDIQ COR
2.1.14.1	Staffing Plan	Plan for staffing, including key personnel, roles, and responsibilities, security clearances, and training.	Initial 30 days after Transition-In Task Order award; Final 90 days after Transition Task-In award.	IDIQ COR
2.1.14.1	HCE Inventory Report	HCE Inventory: Equipment (i.e. hardware): manufacturer, model number, description, installation date, location Cloud services: CSP, service type, description, capacity Software: application, system, owner, software type, description, type of license (e.g., enterprise, single site), version, cost, date of acquisition, date of installation, and anticipated end of software assurance date	Initial 30 days after Transition-In Task Order award; Final 90 days after Transition Task-In award.	IDIQ COR IDIQ CO
2.1.6	Contractor Policies and Procedures	Contractor policies and procedures that cover the operation of the HCE including: • Software patch release and management; • Compliance with ITIL Version 4-aligned configuration management (CM) processes and procedures • Framework processes and procedures describing how the contractor will operate all aspects of the HCE • Security • Equipment installation and maintenance • HCE management and reporting	60 days after Transition Task Order award with updates as Required.	IDIQ COR
2.1.14.1	Transition-In Inventory of computing resources	Inventory of computing resources - servers, storage, & software at transition-in.	60 days of Transition- in Task Order award.	IDIQ COR
2.2.1.1	Vulnerability Assessment Plan	Plan for assessing security vulnerabilities within the HCE.	60 days after Transition-In Task Order award with annual review and update.	IDIQ COR, ISSM, ISSO

PWS Section	Deliverable	Description	Due	Delivered To
2.2.4	Risk Management Plan	The master control document that describes the procedures that are to be used to manage risk throughout the contract and control delivery of the DHS solution.	Initial 60 days after Transition-In Task Order award with updates as required but at least annually.	IDIQ COR ISSM, ISSO
2.2.5	Common Controls Catalog	Documents Contractor implementation procedures and relevant SOPs for compliance to NIST SP800-37 and DHS 4300A and other relevant guidelines.	Initial 60 days after Transition-In Task Order award with annual updates.	IDIQ COR ISSM, ISSO
3.6	Quality Management Plan	Describes the Contractor's organization, processes, procedures, and product controls that the Contractor shall use to make sure the Contract monitors, maintains, and improves quality in delivering HCE performance in accordance with specified Service Level Agreements (SLAs). SLA measurement procedures are to be included in the Quality Management Plan	60 days after Transition Task Order award with annual review and updates as appropriate.	IDIQ COR
6.4.1	Business Continuity Plan	The Business Continuity Plan (BCP) documents plans and procedures for maintaining support during an emergency, including natural disasters and acts of terrorism.	60 days after Transition-In Task Order award with annual updates.	IDIQ COR
6.4.2	Contingency Plans	Contingency Plans (CPs) shall be developed and maintained for all HCE GSS systems.	Initial within 60 days of Transition-In Task Order award; annual updates, by the anniversary date of each GSS ATO.	ISSM, ISSO, IDIQ COR
6.4.3	Patch Management Plan	Description of the Patch Management plan and end to end patching procedures.	Initial within 60 days after Transition-In Task Order award with annual updates or 30 days after any major Change.	IDIQ COR, ISSM, ISSO
6.4.4	Anti-Virus Management Report	Report on the anti-virus implementation and version status of all managed and monitored computing systems in the HCE.	Initial within 60 days after Transition-In Task Order award with Monthly updates (or as required).	IDIQ COR, ISSM, ISSO
6.4.5	General Support System (GSS) - System Security Plan	System Security Plan (SSP) for each GSS system in the HCE.	Initial within 60 days after Transition-In Task Order award; updates within 30 days of any major infrastructure change or new system introduction; updates annually.	IDIQ COR, ISSM, ISSO
6.4.7	Government Furnished Equipment Report	Provides a detailed and updated accounting of all Government Furnished Equipment (GFE), such as equipment, software, and other data in the Contractor's custody.	Initial within 60 days after Transition-In Task Order award with monthly updates.	IDIQ COR
6.8	Catalogs	Provide and maintain a catalog for publicly available prices on COTS Equipment & Software, Infrastructure as a Service (IaaS) and Professional Services.	within 60 days of Transition-in Task Order Award Implement catalogs allowing online ordering.	IDIQ CO IDIQ COR
6.8	Catalog User Guide	Provide operating instructions for end users for accessing and utilizing the catalog(s)	Within 60 days of Transition-In Task Order award.	IDIQ CO IDIQ COR
2.1.1	Service Offerings list	Details and describes services offered to DHS.	Initial within 90 days of Transition-In Task Order Award; As needed within 30 days of changes to service offerings.	IDIQ CO IDIQ COR

PWS Section	Deliverable	Description	Due	Delivered To
2.1.14.2	IDIQ Exit Transition Strategy Plan	Roadmap to enable Contractor to smoothly transition the DC1 contract's personnel, hardware, software, and maintenance to a new Contractor or DHS	90 days after Transition-In Task Order award with updates as required.	IDIQ CO IDIQ COR
2.1.1	Program Status Review Meeting/Report	Provides status information, as mutually agreed to by the contracting parties, of DHS operations and program, technical, and other types of activities for the previous week.	Weekly. Reviewed in status meeting with the COR and uploaded to the Information Repository.	IDIQ COR for entire report; Task Order COR for Task Order portion
2.1.8	HCE: Dashboard Update	Dashboard content includes: • Inventory of all instances, services, and products available in HCE. • Summary of usage information and performance vs. SLAs • DHS Multi-tenant support • Automated provisioning of base template • Approval process before provisioning Deprovision / Decommissioning process • Billing per Component start/stop and reboot VM • Role based permission and access • Performance metrics	Weekly updates to Dashboard status data with notification to the COR and CO of availability.	IDIQ CO IDIQCOR
3.2	Root Cause Analysis Report	Report describing the incident(s) that led to the creation of a "problem" case; root-cause analysis that ensued; and the "solution" to be implemented.	Draft within 24 hours of incident resolution; final upon completion of the Root Cause Analysis (within 72 hours), for all Severity 1 and 2 incidents.	IDIQ COR and Task Order COR
3.3	Configuration Management Database	Database containing the complete HCE hardware and software asset inventory	Monthly, delivered via Dashboard with notification to the COR.	IDIQ COR
3.3	Validated Inventory	Fully validated inventory of all equipment, applications and system software.	Delivered at 4-month intervals as Dashboard accessible and as a downloadable data file with notification to the COR.	IDIQ COR
6.4.6	Security Plan (SP)	Security Plan describing system sensitivity, criticality, security controls, policies, and procedures based upon the completion of the DHS FIPS 199 workbook for each GSS in the HCE.	As required by the SELC; annual review and update.	IDIQ COR, ISSM, ISSO
6.5.1.1	Financial Reports	Monthly Financial Report including all CLIN and catalog purchases to be delivered as processable data available for download from a dashboard.	Monthly Information Repository Update with notification to the IDIQ COR of completion.	IDIQ COR
6.5.1.2	Program Report	Provides status information, as mutually agreed to by the contracting parties, of DHS operations and program, technical, and other types of activities for the previous month.	Monthly Information Repository update with notification to the IDIQ COR of completion with continuous updates to status Dashboard displays throughout the month.	IDIQ COR
6.5.1.3	Contractor Personnel Summary List	Provides the current list of EOD personnel, roles and responsibilities.	Monthly Information Repository update with notification to the IDIQ COR of completion.	IDIQ COR
6.5.2	Capacity Management Report	Display information relating server utilization, storage utilization, network utilization, IaaS utilization, and floor space utilization for physical locations for the previous quarter with a forecast for the next 12 months.	Quarterly Information Repository update with notification to the IDIQ COR of completion.	IDIQ COR

PWS Section	Deliverable	Description	Due	Delivered To
6.5.3	Service Level Agreement Level of Service Report	Provides level of service information as related to each SLA for the previous quarter including an SLA incentive/disincentive evaluation report.	Quarterly Information Repository update with notification to the IDIQ COR and Task Order COR of completion.	IDIQ COR and Task Order COR
6.5.4	Service Quality Report (SQR)	Report addressing new business requirements and activities that affect system or service availability and delivery and a historical view of operations, service and system availability, and trends in service delivery.	Quarterly Information Repository update with notification to the IDIQ COR and Task Order COR of completion.	IDIQ COR and Task Order COR

12 Performance Requirements Summary

The following table lists performance requirements. Each Service Output corresponds to an SLA. Unless specified otherwise, the measurement period for each will be monthly.

Service Output	Performance Objective	Acceptable Quality Level (AQL)
1	Service Desk: Speed to Answer. Speed to answer Service Desk calls in 45 seconds or less.	95%
2	Service Desk: Speed to Respond to Communications. Speed to respond to contacts through identified communication channels other than telephone (currently email) in 1 elapsed hour or less.	95%
3	Customer Satisfaction Rating. Overall measure of the Net Promoter Score (NPS) measured monthly is greater than or equal to 30. Service Satisfaction rated as "Very Satisfied" or "Extremely satisfied" measured quarterly. 94% of responses rating 8.0 or better on a survey scale of 1 to 10.	NPS ≥ 30 94% ≥ 8.0
4	Root cause determination. The percentage of Severity 1 and Severity 2 Incidents for which Root Cause Analysis (RCA) has been completed and submitted within 72 hours of Incident occurrence.	95%
5	Incident Management Resolution Time (Severity 1, 2, and 3). Elapsed time to resolve incidents for Severity 1, 2, and 3 incidents occurring during a reporting period measured in continuous elapsed time from the time of incident occurrence - not in business hours. Severity 1 - 4 Clock Hours (240 Minutes); Severity 2 - 8 Clock Hours (480 minutes); Severity 3 - 12 Clock Hours (720 minutes)	99.5% per Severity Level
6	Incident Management: Time for DHS System Owner to be notified when non-security incident is found. Target elapsed time for System Owner and designated stakeholder notification for Severity 1 and 2 incidents is 30 minutes or less; notification time for Severity 3 incidents is 8 hours for a reporting period.	95%

Service Output	Performance Objective	Acceptable Quality Level (AQL)
7	Incident Management: Status Update Frequency. Incident tickets for Priority Level 1 and Level 2 incidents are to be updated at least hourly. Priority Level 3 incidents are to be updated every 8 hours. All other incident tickets shall be updated at least daily. Measurement is for all tickets during a reporting period.	99.5% per Priority Level
8	Service Asset and Configuration Management: Percentage of CMDB Inventoried Annually - Accuracy of Level 1 and 2 Systems. Percentage of Level 1 and 2 Systems found to have accurate information in the CMDB measured annually with an error rate less than or equal to 2%.	98%
9	Service Asset and Configuration Management: Percentage of CMDB Accuracy of Level 1 and 2 Systems. Percentage of Level 1 and 2 systems found to have accurate information in the CMDB in a reporting period. Validation is based on a 25% minimum progressive sample of the baseline inventory measured monthly to ensure a 100% audit over four months with less than 2% error rate.	98%
10	Service Asset and Configuration Management: Percentage of Contractor provided and/or managed physical and virtual assets and cloud services inventoried. Validation that at least 10.00% of baseline inventory of physical and virtual assets and cloud services within the HCE was progressively audited during a monthly reporting period to ensure a 100% validation over 10 months with an error rate not to exceed 0.5%.	99.5%
11	Change Management: Percentage of Successfully Implemented Changes - Level 1 and 2. Percentage of Changes authored and primarily executed by the Contractor for Level 1 and 2 supported systems in data centers, colocation facilities, and cloud environments that did not result in an incident or fault and with no negative impacts to operational stability.	99.5%
12	Change Management: Percentage of Changes Resulting in an Incident. Percentage of Incidents per reporting period that were the result of Changes authored and/or primarily executed by the Contractor.	$\leq$ 3%

Service Output	Performance Objective	Acceptable Quality Level (AQL)
13	Change Management: Percentage of Emergency Changes. Percentage of Contractor initiated non-security changes that were flagged as "Emergency" compared to all other rendered changes.	≤ 10%
14	Capacity Management: DHS CPU Utilization. Percentage of CPU Utilization for Contractor provided and/or managed Level 2 systems or applications. (average [mean] percentage for each system and application).	≤ 70%
15	Capacity Management: DHS Disk Utilization. Percentage of System Disk Utilization - Level 2 systems. Average (mean) Percentage of disk Utilization for Contractor-provided and/or Level 2 systems.	≤ 70%
16	Capacity Management: DHS SAN Utilization. Percentage of SAN Utilization - Level 2 Systems. Average (Mean) Percentage of SAN Utilization of Contractor-provided and/or managed Level 2 Systems.	≤ 70%
17	Capacity Management: DHS Network Bandwidth Utilization. Percentage of LAN bandwidth utilization of Contractor provided and/or managed DHS HCE Network Infrastructure. - Reporting Period Average (Mean) Percentage of Network Utilization of Contractor provided and/or managed DHS HCE infrastructure (enterprise).	≤ 70%
18	Capacity Management: HCE CSP Compute Resource Utilization. Average Percentage Utilization of CSP-Resources provided by the Contractor during the reporting period (average (mean) percentage) does not exceed the AQL.	≤ 85%
19	Capacity Management: HCE CSP Storage Resource Utilization. Average Percentage of Storage Resource Utilization for CSP storage resources provided by the Contractor during the reporting period does not exceed the stated AQL.	≤ 85%
20	Capacity Management: HCE CSP Database Resource Utilization. Percentage of Database Resource Utilization - Level 2 Systems. Average (Mean) Percentage of Database Resource Utilization of Contractor- provided and/or managed Level 2 Systems.	≤ 85%

Service Output	Performance Objective	Acceptable Quality Level (AQL)
21	Availability Management. Percentage of System Availability. Percentage of availability per reporting period for Contractor-provided and/or managed Level 1 and 2 systems, including cloud services. Reporting Period Average (mean) percentage of System availability for Contractor-provided Level 1 and 2 Systems, including cloud services.	99.9%
22	Availability Management: Percentage of LAN Availability. Percentage of availability per reporting period for Contractor-provided and/or managed LAN services. Reporting period average (mean) percentage of LAN availability.	99.9%
23	Backup Success Rate. Reporting Period Backup Success Rate Average (mean).	99.5%
24	Disaster Recovery Planning, Testing, and Auditing. Percentage of completed Disaster Recovery documentation (e.g., Security Authorization artifacts) and/or support for stakeholders that have the following: 1) a complete documented DR plan updated annually, 2) initial and annual successful system recovery tests performed.	100%
25	Security Management: Security Intrusion Detection. Percentage of Contractor managed Intrusion Detection System (IDS) sensors that successfully generate an alert for events during the reporting period.	100%
26	Security Management: Intrusion Reporting and Compliance. Percentage of "significant" Level 1 and Level 2 Security Incidents reported immediately (i.e., within 30 minutes) to System Owner and organizational stakeholders for the measured reporting period.	100%
27	Security Management: Access Termination. All physical/logical access removal administrative actions and notifications shall be submitted within 6 business days of employee termination. However, if employee is terminated within 3 business days of closing month, Contractor security management personnel have until the 3rd day of following month to meet the SLA.	100%

Service Output	Performance Objective	Acceptable Quality Level (AQL)
28	Security Management: Vulnerability Scan Compliance. Percentage of Level 2 systems having no "moderate or above" vulnerabilities or are within the published "Comply Date" (if no Comply Date provided, default is 30 days), or have approved DHS mitigation.	99.00%
29	Security Management: Security Authorization Compliance: Percentage of systems, applications and services for which the Contractor provides Security Authorization (SA) artifacts to ensure the SA package is up to date (i.e., ATO has not expired). Percentage of current, up-to-date SA packages for systems where the supplier is responsible for the SA packages and artifacts.	100%
30	Security Management: Virus Protection Management Compliance. Percentage of Contractor supported systems or applications with current anti-virus signatures.	100%
31	Security Management: Information Security Awareness Training Compliance. Percentage of Contractor employees having received DHS Security Authorization Training for the measured reporting period. Percentage of Contractor employees supporting the HCE Task Order having documentation demonstrating completion of Information Security Awareness Training for the measured reporting period.	100%
32	IaaS: Service Availability. Percentage of IaaS availability in the reporting period.	99.9%
33	IaaS: Service Provisioning Time. Elapsed time taken to provision each virtual machine with the basic operating system.	8.0 Hours
34	IaaS: Service De-Provisioning and De-Commissioning Time. Elapsed time required to de-provision or de-commission each instance (VM).	8.0 hours

Service Output	Performance Objective	Acceptable Quality Level (AQL)
35	Security Integrity - Successful System Scans Compliance. Assesses the ability of the Contractor to conduct successful system Vulnerability and Antivirus scans. Measures the number of successful system Antivirus and Authenticated and non-authenticated Vulnerability scans conducted during the reporting period compared to the total number of appliances, applications, devices, environments, solutions, or servers subject to each scan.	99.9%
36	Remediation - Vulnerabilities mitigated or remediated within 30 days.	99.5%
37	Network Services: Availability of the HCE Network Infrastructure - The aggregated availability of HCE network infrastructure during the reporting period.	99.9%

Appendix A. Applicable Documents

Compliance Documents

The following documents provide specifications, standards, or guidelines that must be complied with in order to meet the requirements of this contract:

- DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, January 6, 2005. https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_110421_safeguarding_sensitive_but_unclassified_information.pdf
- DHS Instruction Manual 047-01-007, Revision 3, Handbook for Safeguarding Sensitive Personally Identifiable Information (PII), December 4, 2017. https://www.dhs.gov/sites/default/files/publications/Handbook%20for%20Safeguarding%20Sensitive%20PII_0.pdf
- DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017. https://www.dhs.gov/sites/default/files/publications/Sensitive%20Systems%20Policy%20Directive%204300A.pdf
- DHS 4300A Sensitive Systems Handbook (and attachments), Version 12.0, November 15, 2015. https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf
- DHS Privacy Incident Handling Guidance DHS Instruction Guide 047-01-008, December 4, 2017. https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf
- DHS System Security Authorization Guide V11.1, March 16, 2015. https://www.dhs.gov/sites/default/files/publications/Security%20Authorization%20Process%20Guide_1.pdf

Reference Documents

This requirement should ensure alignment with Federal and Department-wide IT policies and strategies. Specific policies, strategies, and guidance include:

- NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, September 2020.
- NIST Special Publication (SP) 800-53A, Rev 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans," December 2014, updated December 18, 2014.
- NIST Special Publication (SP) 800-61, Revision 2, Computer Security Incident Handling Guide, August 2012

See: https://www.nist.gov/publications.

Directives and Standards

The following standards apply to all DHS processing. DHS reserves the right to approve or disapprove any variances to standards.

Information Security Standards

- National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
- NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, September 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
- Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, May 25, 2001, https://csrc.nist.gov/publications/detail/fips/140/2/final
- NIST Special Publication 800-53A Rev 4, Guide for Assessing the Security Controls in Federal Information Systems, December 18, 2014, https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
- FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006, https://csrc.nist.gov/publications/detail/fips/200/final

List of Acronyms

Acronym	Definition
ACR	Accessibility Conformance Report
AIX	IBM Advanced Interactive eXecutive
API	Application Programming Interface
AQL	Acceptable Quality Level
ATO	Authority to Operate
BCP	Business Continuity Plan
BI	Background Investigation
CBP	U.S. Customs and Border Protection
CCSP	Certified Cloud Security Professional
CentOS	Community Enterprise Operating System
CISA	Cybersecurity and Infrastructure Security Agency
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CLIN	Contract Line Item Number
CM	Configuration Management
CMDB	Configuration Management Database
COMSEC	Communications Security
CONOPS	Concept of Operations
COR	Contracting Officer's Representative
CP	Contingency Plan
CPSL	Contractor Personnel Summary List
CSO	Contractor Security Officer
CSP	Cloud Service Provider

Acronym	Definition
CSPL	Contractor Personnel Summary List
CWMD	Countering Weapons of Mass Destruction Office
DAC	Discretionary Access Control
DC1	Data Center 1
DCCO	Data Center and Cloud Optimization
DHS	Department of Homeland Security
DR	Disaster Recovery
DUNS	Data Universal Numbering System
EDMO	Enterprise Data Management Office
EIT	Electronic and Information Technology
EOD	Entry on Duty
ESOC	Enterprise Security Operations Center
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FLETC	Federal Law Enforcement Training Centers
GFE	Government Furnished Equipment
GIAC	Global Information Assurance Certification
GCSA	GIAC Cloud Security Automation
GSS	General Support System
HCE	Hybrid Computing Environment
HQ	Headquarters
HSEN	Homeland Security Enterprise Network
I&A	Office of Intelligence and Analysis
IaaS	Infrastructure as a Service
IaaS-DC1	Infrastructure as a Service-DC1

Acronym	Definition
IBM	International Business Machines Corporation
ICD	Intelligence Community Directive
ICE	U.S. Immigration and Customs Enforcement
ICT	Information and Communications Technology
IDIQ	Indefinite Delivery Indefinite Quantity
IDS	Intrusion Detection System
IPS	Intrusion Protection System
ISO	Industrial Security Office
ISSA	Industrial Security Staff Approval
ISSO	Information System Security Officer
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Validation and Verification
LAN	Local Area Network
LPR	Lawful Permanent Resident
MD	Management Directive
MGMT	Management Directorate
MPR	Monthly Program Report
NAS	Network Attached Storage
NASA	National Aeronautics and Space Administration
NCCIPS	National Center for Critical Information Processing and Storage
NDA	Non-Disclosure Agreement
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Science and Technology
NOSC	Network Operations and Security Center

Acronym	Definition
NPS	Net Promoter Score
O&M	Operations and Maintenance
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCISO	Office of the Chief Information Security Officer
OCPO	Office of the Chief Procurement Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OSI	Office of Security and Integrity
P&E	Planning & Engineering
PaaS	Platform as a Service
PCII	Protected Critical Infrastructure Information
PDD	Position Designation Determination
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PM	Program Manager
PMP	Program Management Professional
POA&M	Plan of Action and Milestones
POC	Point of Contact
PRS	Performance Requirements Summary
PTA	Privacy Threshold Analysis
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
QMP	Quality Management Plan

Acronym	Definition
RA	Risk Assessment
RCA	Root Cause Analysis
RHEL	Red Hat Enterprise Linux
S&T	Science and Technology Directorate
SA	Security Authorization
SAN	Storage Area Network
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDK	Software Development Kit
SDM	Service Delivery Manager
SLA	Service Level Agreement
SLO	Service Level Objective
SOC	Security Operations Center
SOP	Standard Operating Procedure
SORN	System of Records Notification
SP	Security Plan
SPII	Sensitive Personally Identifiable Information
SQR	Service Quality Review
SSI	Sensitive Security Information
SSN	Social Security Number
SSP	System Security Plan
ST&E	Security Test and Evaluation
TB	Terabyte
TCO	Total Cost of Ownership
TRM	Technical Reference Model

Acronym	Definition
TS	Top Secret
TSA	Transportation Security Administration
UCS	Unified Computing System
URL	Universal Resource Locator
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	U.S. Secret Service
VC	Virtualization Center
VM	Virtual Machine
WAN	Wide Area Network
WCAG	Web Content Accessibility Guide
WPaaS	Workplace as a Service