Management Directorate

IT Services and Operations

Headquarters Operations Division

HOD Projects & IT Service Delivery Task Order Statement of Work DSS 2.0 BPA

February 16, 2021

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 General Information

1.1 Scope

The Headquarters Operations Division (HOD) IT Service Delivery Task Order provides effective operational and management solutions to facilitate the sustainability and administration of the Information Technology (IT) systems in support of the DHS Headquarters (HQ) component mission requirements. These solutions increase the productivity of end users, engineers, mission support personnel, administrative users, and all Components in support of DHS's overall mission by quickly and efficiently delivering reliable, innovative, and secure IT services. The Information Technology Operations (ITOPS) Headquarters Operations Division (HOD) oversees this Task Order and the portfolio of services and capabilities associated with the end-user services domain; this includes defining and executing overall strategy, roadmaps, standards, policies, investments, and projects.

The Contractor shall perform the services listed below for the functional areas and ensure the services are integrated, well defined, documented, standardized, repeatable, accurate, and timely. All the associated processes in all functional areas shall produce secure, high-quality and cost-effective services, work products, and IT solutions, and shall be properly documented leveraging the ITIL v4 framework. The Contractor shall perform these services in a manner that will drive efficiencies through continual maintenance and improvement of documented processes.

This document is intended to support the government's requirement for the following services under the DHS Desktop Support Services BPA:

- Task 1: Program Management Services
- Task 2: IT O&M Services
- Task 3: Business Transformation and Innovation Services

Task Order (TO) requirements that are designated as *Optional* should be considered severable and only performed if funding is provided.

1.2 Period of Performance

Task Order Period	**Ordering Period**
Base Period	3/2/2021 – 3/1/2022
Option Period One	3/2/2022 – 3/1/2023
Option Period Two	3/2/2023 – 3/1/2024
Option Period Three	3/2/2024 – 3/1/2025
Option Period Four	3/2/2025 – 3/1/2026

1.3 Place of Performance

The work will be performed in the National Capital Region (NCR), to include Mt. Weather, locations across the Continental United States (CONUS) at sites such as national/state fusion centers, state, local,

and tribal centers, and designated remote locations. Additional support locations include some outside CONUS (OCONUS) locations such as Hawaii, Guam, and potentially non-US locations.

1.4 Telecommute Authority

Permanent telework may only be authorized by the Contracting Office Representative (COR) or Contracting Officer (CO). Situational telework may be authorized by the government's designated task order lead or alternate representative.

1.5 Hours of Operation

The Contractor shall provide support 7 days a week, 24 hours a day, 365 days a year (24x7x365). The Contractor's support shall include solutions for coverage during Core Business Hours, Non-Core Business Hours, and Holidays. Hours of operation vary by Task and are identified within each Task or Subtask description.

- Core Business Hours:
  - Support rendered during the Government's normal hours of operations, between 6:00 a.m. to 6:00 p.m. local time weekdays, Monday through Friday, excluding Federal Holidays.
- Non-Core Business Hours:
  - Support rendered during any period of time other than the hours of 6:00 a.m. to 6:00 p.m. local time weekdays, any support rendered Saturday and Sunday, 24 hours a day, or any support rendered during Government closures to exclude Federal Holidays.
- Holiday Hours:
  - Support rendered during any and all Federal Holidays.

1.6 Travel

If travel is required, it must be authorized with prior Contracts Officer (CO) or Contracts Officer Representative (COR) written approval and in accordance with the Federal Travel Regulations (FTR).

1.7 Applicable Appendices and Documents

The following documents provide information that is applicable to this TO:

- **Appendix A Acronyms and Abbreviations**
- **Appendix B Service Level Agreements**
- **Appendix C DHS HQ and Customer Supported Sites**
- **Appendix D Executive VIP (EVIP) and VIP Position List**
- **Appendix E FCR Incident List**

2 Specific Objectives/Tasks

2.1 Task 1: Program Management Services

Program Management facilitates all TO services and operations management functions. It involves transition, implementation, oversight and administration of services and operations and maintenance of core tasks. The goal of program management is to:

1. Organize management of integrated IT services and projects
2. Provide cost and budget management
3. Ensure continued service delivery in accordance with the service level requirements, regardless of changing or fluctuating workload or personnel availability
4. Improve processes by facilitating performance planning and alignment
5. Drive business and operational process standardization
6. Document business and operational processes

The objective is to provide program management activities, reporting and other general contract management services needed to achieve the cost, schedule and performance goals under the TO.

Program Management Services shall ensure the Contractor:

- Develops and executes Transition-In/Transition-Out plans
- Provides a business model for ensuring that the Government's requirements are met
- Provides Quality Assurance and Surveillance
- Recommends new technologies and processes to ITO HOD throughout the life of the (TO) to ensure delivery of the best value products or services
- Maintains and updates the documentation in a centralized, government-designated repository. The Contractor shall manage the current environment, adding new functionality and updating existing data as needed or at the Government's direction
- Incorporates all service level, metrics, and performance standards

2.1.1 Subtask 1: Program Management

The Contractor shall develop and implement a Program Management Plan (PMP) to provide program management support while adhering to DHS policies and guidelines, which includes the management and oversight of all activities performed by Contractor personnel, including the effective use of subcontractors to satisfy the objectives and service level requirements identified in this contract.

The PMP shall include:

- Methods for managing key elements of the technical approach, resources, communication, assumptions, risk, and schedule
- Strategies for managing Task level activities, deliverables, critical dependencies, and milestones
- Description of the data to be collected to support service level and performance management and how often that data will be collected
- Escalation Processes and Procedures

- Ticket Management Lifecycle
- Quality Assurance Management

The Contractor shall provide PMP updates annually, following the exercise of optional services that require operations and maintenance services, or as changes are required. The Plan shall include a comprehensive breakdown of how delivery oversight, program management, and planning will be completed. It shall detail how the Contractor will accomplish the requirements within this TO and how the Contractor will accomplish through service level agreement management and metrics analysis for each of the objectives presented.

2.1.1.1 Quality Assurance Management

The Contractor shall develop and implement a Quality Assurance Program aligned to the overall objectives of the TO. The Contractor shall ensure all communications and work products are accurate, complete, compliant, and submitted in a timely fashion and all work products are compliant with DHS HQ standards and submitted on schedule to the Government as client-ready deliverables.

2.1.1.2 Records Management

The Contractor shall develop, organize, and maintain a records management process that adheres to DHS HQ policies and guidelines in conducting and implementing records management processes and that fulfill the requirements of Federal law and policy for records management associated with the scope of the contract. The Contractor shall utilize a Government-owned and designated centralized repository. All documentation created under this contract is Government owned. The Contractor is to ensure that work products or artifacts are not marked "Proprietary", "Company Confidential", or with any other non-Government restrictive language, including the use of corporate logos.

2.1.1.3 Communications Management

The Contractor shall include a Communications Plan within the PMP that results in proactive and timely information sharing to relevant federal and contractor stakeholders for objectives to be met, and decisions made in a timely manner. This Plan shall include providing the work products listed in Table 4-1 Contract Deliverable Requirements List, as well as participation in Government sponsored meetings.

2.1.1.3.1 Government Sponsored Meeting Support

The Contractor shall attend Government sponsored meetings in -person or virtually through LAN-A approved software. The purpose is to ensure effective and efficient distribution of information, remediate any possible coordination issues, and to facilitate communication related to this procurement and other related DHS procurements. The meetings may include:

- **Daily Operations Meetings**. These meetings will occur on business days and include contractors representing various DHS projects. The Contractor shall participate in a daily operations meeting with the Government via teleconference to discuss IT service-related activities, provide a status on outstanding risks and issues, and coordinate services with both government and contractor staff.
- **Weekly Meetings**. These meetings will occur weekly and include contractors representing various DHS IT projects. The Contractor shall meet weekly with designated government staff to

discuss engineering, operational, service, and/or project related status or issues. Service-related details to be discussed include performance compliance, service levels, and metrics analysis related to service delivery.

- **Program Review Meetings**. The Contractor shall plan and facilitate program review meetings with the Government COR/PMO/Management. Topics for discussion will include: contract financial status, contract performance metrics, mitigation plans for under-performing areas, and the status of other risks, issues, problems, and concerns and proposed solutions. The briefing shall be a high-level presentation of information already discussed in previous meetings and presented in other reports. The Contractor shall provide the government with presentation materials for review three (3) business days prior to the briefing.
- **Ad Hoc Meetings**. The Government may require the Contractor to participate in ad hoc meetings to discuss any contract related service, activities, issues, or concerns. These meetings may be with Government representatives only or may be attended by other contractors providing IT services to DHS.

2.1.1.4 Performance Management

The Contractor shall ensure compliance with the agreed upon performance measures. This objective also includes providing a performance management approach to meet or exceed the service level requirements described in Appendix B: Service Level Agreements (SLAs). The contactor shall provide a Quality Assurance and Surveillance Plan (QASP) detailing how SLAs will be measured and tracked. The QASP shall detail the contactor's approach to service-level management including performance planning, performance measurement, performance analysis and reporting, performance correction and continual service improvement.

2.1.1.5 Financial Management

The Contractor shall provide financial management services at the TO level to include:

- Cost estimates for changes to TO requirements and/or specifications
- Monthly and annual billing invoices for services rendered
- Support for Government financial auditing requests
- Financial forecast modeling to include, but not limited to, burn charts and Estimate at Complete (EAC) information
- Contract Line Item Number (CLIN) summary table to include funding due dates and relevant milestones

2.1.1.6 Business Continuity

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 15 business days after the date of 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 description of workflow for implementing Automated Call Distribution procedures
- A list of primary and alternate Contractor points of contact, each with primary and alternate

Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within four (4) 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 located 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 this contract.

All personnel supporting this Task Order shall be categorized as Essential and shall continue to provide support during Government shutdowns and other government designated events. The Contactor shall ensure continuity of service during Government shutdowns, executing the business continuity plan, as required.

2.1.1.7 Contractor Training

The Contactor shall adhere to all DHS HQ contractor training requirements. This includes the completion of DHS Insider Threat Training and DHS Cybersecurity Awareness Training (CSAT)/Rules of Behavior Training which shall be completed within the requisite due date. In certain circumstances the Contractor shall also be required to complete training for special rights (DHS Privilege User Training) or for access to classified space/data (SCI Annual Refresher Training).

2.1.1.8 Service Integration Support

The Contactor shall provide service integration support to ensure all Task Order resources are adequately prepared and trained for new technology/tool deployments or IT environmental changes. The Contactor shall develop a wholistic and repeatable approach to validate the operational readiness across all personnel/tiered support to ensure a seamless handoff between project engineering and O&M sustainment teams. This approach should include participation in IPTs, documentation creation/validation, (e.g. SOPs, work instructions) and training of contractor staff.

2.1.2 Subtask 2: Transition Management

The Contactor shall provide transition-in/transition-out services to support task order award and close-out tasks. Transition-In shall begin sixty (60) days prior to beginning of the base period. Transition-In/Transition-Out shall be transparent and seamless to the users with no degradation or breaks in service availability while maintaining existing security, service quality, contract support, performance levels, and an orderly transition of assets.

2.1.2.1 Transition-In Management

Transition-In shall be completed within sixty (60) days from contract effective date and the Contractor will coordinate and integrate the Task Order transition-in tasks with the current Contractors' transition-out tasks. Transition activities include the transfer of privileged account passwords, proper documentation of all IT assets, and the issuance of Government-Furnished Equipment (GFE).

The Contractor shall provide a Transition-In Plan no later than ten (10) days following the Task Order Award Date. The Transition Plan shall include:

- Project plan for all transition activities
- Resources required for transition, transition activities, and management activities
- Gap analysis on as-is and to-be functions and processes
- A description of how knowledge transfer will be conducted to achieve transition objectives (e.g. shadowing, training sessions, standard operating procedures, reference guides, etc.)
- Identification of any known risks, foreseeable problems, and identification of additional resources and/or cost: if any, that will be required to mitigate those risks and ensure a successful transfer of responsibility
- Quantification of risk in days or weeks of delay and the optimistic, pessimistic, and most likely outcome for the program considering identified risks
- Identified assumptions and dependencies
- An Integrated Master Schedule (IMS) that identifies tasks and objectives to be transitioned, milestones and estimated completion dates

Transition-In shall be deemed complete as of the first business day immediately following the service transition completion as specified in the Transition-In Plan. The Government will confirm acceptance with a written notice accepting transition-in completion. As of the Government Transition-In service acceptance date, the Contractor shall have successfully completed implementation and deployment of all required Transition-In activities.

2.1.2.1.1 Transition-In Post-award Kickoff Meeting

The Contractor shall participate in a post-award kickoff and introduction meeting with Government representatives within fifteen (15) calendar days after TO award in the Washington DC area. The Contractor will be required to provide a presentation introducing its team members and to give a brief synopsis of the team's Transition-In Plan. The exact time and location will be determined at time of the TO award.

2.1.2.2 Transition-Out Management

The Contractor shall develop and implement a Transition-Out Plan to the successor contract. The transition shall be transparent and seamless to the users with no breaks in service availability while maintaining existing security, service quality, contract support, performance levels, and an orderly transition of assets. Transition-out tasks shall be coordinated, integrated, and initiated with the successor Contractor transition-in tasks prior to the end of the period of performance and with sufficient time to meet the stated objective.

Prior to the completion of the transition-out activities, the Contractor will transfer all GFE back to the Government.

The Contractor shall plan for and provide a transition-out period not to exceed ninety (90) days at the TO level. Transition out shall be available in the final option period of the TO as well as at the end of the base and each option period. At a minimum, transition out services shall include the following:

- Development of a Transition-Out Plan for transferring service responsibility from this award to another provider or back to the DHS HQ and its Components. The transition plan shall identify what actions the Contractor and the DHS HQ and its Components must perform, to smoothly transfer information, data, government-furnished property and any management responsibility to another party. The transition plan shall address any known risks, foreseeable problems, and shall identify the additional resources and cost, if any, required to mitigate these risks and ensure a successful transfer of responsibility.
- Carrying out the actions in the Transition-Out Plan and managing the completion of those tasks to ensure successful transfer of all responsibilities by the agreed upon transition service acceptance date as specified in the call.
- Delivering to the DHS HQ and its Components all agency related account, inventory, invoice, and other data resident in the Contractor's data system necessary to enable another provider, or DHS and its Components, to assume service responsibility. This information shall include all information that the Contractor works with to manage the agency's accounts, service delivery, and equipment. All data shall be delivered, available, and accessible to the DHS HQ and its Components in electronic format to enable electronic transfer into other data systems. The specific format(s) for the data will be specified at the TO level during transition. This information will be referred to as Agency Transition Data.
- Upon expiration of the TO calls, as part of its close-out responsibilities within FAR Part 4.8, the Contractor shall continue to support the DHS HQ and its Components in handling and tracking disputes on or before the TO call expiration date through final resolution, or for six (6) months after expiration, whichever is less. (These are not contract claims as defined in FAR Part 33, which will be handled by a warranted CO.)

The Transition-out Plan details shall address, at a minimum, the following:

- Continuity of Services in accordance with Information Technology Infrastructure Library (ITIL)(v4) framework
- Contractors plan to close-out all open tickets

- Coordination plan for the incoming Contractor and/or Government personnel to transfer knowledge via weekly status meetings regarding:
    - Project management processes
    - Points of contact
    - Location of technical and project management documentation
    - Physical inventory
    - Status of ongoing technical initiatives
    - Contractor-to-Contractor coordination to ensure a seamless transition
    - Schedules and milestones
    - Actions required of the Government

2.2 Task 2: IT O&M Services

The Contractor shall employ the ITIL Service Management Framework (Version 4 or any subsequent revisions) or any comparable framework to guide management of IT O&M services, and the processes, functions, and other capabilities needed to support them.

ITIL-aligned framework provides the structured discipline required to operate and manage HOD IT services. Service Delivery and Service Support processes shall be based on ITIL best practices, and all processes and procedures shall interface and align with comparable HOD processes and procedures. Support services based on ITIL focus on the day-to-day issues to achieve operational goals. These support services shall provide an optimal balance between stability and flexibility of the IT services resulting in improved IT service delivery.

IT O&M Services shall include support for workstations, laptops, tablets, thin clients, software, mobile devices, networked and locally connected peripherals, teleconferencing, operating systems, drivers, client applications, and interfaces to or for any of the devices currently covered and approved by HOD. These services include the installation, movement, maintenance, troubleshooting, and disposition in accordance with the DHS HQ process and procedures.

The DHS HQ location addresses are identified in the Appendix C Supported DHS HQ and Supported Customer Sites. This list shall be maintained by the contractor in the ITSM tool and updated in conjunction with monthly government reviews. The actual numbers and sizes of these sites are provided as a baseline and may vary depending on the requirements of the Government. The Contractor shall address how and where it will regionalize the support structure to minimize travel costs, the activities and tasks addressed at each level of support, and the plans and methods for establishing and maintaining communication with other contractors providing IT services that ensure continuous and effective coordination.

The Contactor shall provide multiple levels of support based on user and/or location type. The support tiers will have varying SLAs as well as different price points allowing the Government to select the appropriate level of support for all users.

The Contactor shall provide on-site support services (or dispatched, if requested) for the defined durations:

Site-Level Support:

- **Normal Business Hour Support:**
  - On-site support provided during the Government's normal hours of operations, between 6:00 a.m. to 6:00 p.m. local time weekdays, Monday through Friday, excluding Federal Holidays.
- **24x7x365 Support:**
  - On-site support provided 24x7x365.
- **Dispatch Only Support:**
  - Provide coordinated, scheduled on-site response during normal business hours.

The contractor shall provide the user level support tiers listed below. Each are aligned with a specific IT Service Desk (ITSD) and End User Services (EUS) SLAs identified in Appendix B Service Level Agreements.

- **Silver = NCR Standard User**

The Silver support tier is comprised of Standard Users. Standard Users are individuals who warrant IT support within the normal day-to-day operations.

- **Gold = NCR Standard User Plus**

The Gold support tier is comprised of Standard Users Plus. Standard Users Plus are individuals—designated in writing by a very important person (VIP)—who have authority to request support on behalf of the VIP. This user is prioritized ahead of a Standard User. Examples of Standard User Plus users are executive assistants and Component IT staff/representative.

- **Platinum = NCR VIP**

The Platinum support tier is comprised of VIP users. The VIP users are Senior Department Executive Level staff who require near-immediate on-site IT support from the Support Staff (all IT functions). VIPs are prioritized ahead of all other support activities. Examples of VIP users are SES or DHS HQ and Component Senior Managers. The VIP list will be reviewed quarterly with updates to be provided to the Contractor.

- **Diamond = NCR EVIP**

The Diamond support tier is comprised of executive very important person (EVIP) users. The EVIP users are Senior Department Executive Level Staff who require immediate on-site IT support from the Support Staff (all IT functions) and are identified in Appendix D Executive VIP Position List. EVIPs are prioritized ahead of VIPs and all other support activities.

- **Non-NCR User Support**

Non-NCR user support is comprised of users who are not located in the NCR. Service locations and levels of support shall be identified upon service order or modifications to the SOW

2.2.1 Sub-Task: IT Service Desk

The Contractor shall provide ITSD support for approximately 27,500 contacts monthly, troubleshooting, resolving, and/or escalating incidents or request with computers and other information technology products. The objective of this sub-task is to:

1. Provide help desk and support services leveraging industry standard service management best practices on a 24x7x365 basis offering phone, self-service, email and live web-chat 7am to 7pm weekdays.
2. Support HOD's trouble ticket tracking system that supports all IT services related to trouble reporting, incident resolution, and request for IT services.
3. Provide A-LAN user account management, such as, creation, modifications, updates, reporting, disabling, enabling, monitoring, and removal.

2.2.1.1 ITSD Ticket Management

The ITSD shall receive, record, process, manage, track, update, resolve, and close all requests for service, incidents, and fulfillment. Service Desk analysts shall answer calls promptly and courteously, identifying themselves by name and following pre-approved scripts. Analysts shall capture all relevant caller information, including caller component and organization, issue/request details, assets in use by and assigned to the caller, and the caller's assigned location.

All tickets must be assigned a priority using the criteria provided in the following table.

Table 2-1 Customer Incident Priority by Definition

Priority	Definition
1 - Critical	• Any issue relating to the safety or health of any Unclassified Local Area Network (A-LAN) user (e.g., fire, electrical short, broken or damaged equipment) • Work stoppage affecting an A-LAN EVIP/VIP • Work stoppage during an actual contingency event or affecting activated Emergency Relocation Group staff
2 - High	• Mission Critical Work Stoppage affecting an entire A-LAN site/location • Mission Critical Work Stoppage affecting multiple A-LAN users • Routine A-LAN EVIP/VIP requests • Work stoppage during a contingency exercise or affecting activated Emergency Relocation Group staff during an exercise
3 - Medium	• Work stoppage affecting an A-LAN user for which there is no workaround
4 – Medium Low	• Work stoppage affecting an A-LAN user for which there is a workaround • Non-critical problem that does not involve a work stoppage
5 - Low	• Routine requests for all other user requirements/requests for service(s)

The Contractor shall provide trained technical support with demonstrable experience identifying, diagnosing, and troubleshooting incidents; following troubleshooting scripts; and resolving and closing incident tickets. Analysts shall be knowledgeable about troubleshooting techniques and shall demonstrate experience and training in the use of a service ticket management system, as applicable. The Contractor shall resolve tickets only after verification from the customer.

The Contractor shall provide escalation support, defined in conjunction with and set forth by the CO or

COR, for all security-related incidents. Service Desk Analysts shall provide the Government with information concerning the source, scope, and effect of all incidents and identify and propose solutions to remediate those incidents, where possible, as requested by the customer.

2.2.1.2 ITSD Incident Management

The Contractor shall provide issue identification and initial incident troubleshooting for all issues received by the ITSD. The Contractor shall assign and update incidents in the Information Technology Service Management (ITSM) tool to address incident status, assigned group, routing, and any constraints to delivery of services.

The Contractor shall create, manage, and use troubleshooting or problem-isolation scripts to expedite and facilitate identification and resolution of known issues. When undocumented issues are identified, the Service Desk Staff shall update the knowledge base and scripts.

The Contractor shall document in Incident tickets the causes of delays outside of the Contractor's control to support SLA waiver requests.

Incidents received by the Contractor that are identified not within the Contractor's scope of work shall be routed to the correct assignment group noting all findings and customer interactions performed on the incident.

The Contractor shall perform analysis of incident tickets to support proactive identification of and quick reaction to issues in the environment. The Contractor shall perform trend analysis on an ongoing basis to identify issues within the production environment for:

- Incidents that have not occurred on a repetitive basis enough to warrant escalation to a Problem ticket but have occurred enough to warrant a potential issue or degradation within a service or product.
- Identify an issue within a process that would require a review in order to correct process or address adherence to the process.
- Warrant the creation of a Knowledge Article (KA), Agency communication, and/or discussion/training with the ITSD to improve first contact resolution.
- Identify a change in end user behavior/actions that would require the government to address acceptable use policies.

ITSD shall assign incident tickets to EUS whenever a customer requests on-site support or when they leave feedback that requires EUS follow-up.

The Contractor shall participate in regular operations meetings with Government stakeholders and the other HOD contractors in order to assure integration of issues and open work.

2.2.1.3 ITSD Service Request Management

The Contractor shall manage all service request fulfillment tasks working in the ITSM tool. When a request is approved (or pre-approved), a fulfillment task will be assigned to the appropriate assignment group. The contractor shall update the task with status and completion information. The Contractor shall work together with the government to define and refine the service definitions that

appear in HOD service request catalog.

2.2.1.4 Tier 0 Self-Service

The Contractor shall design, develop, and maintain self-service capabilities to drive faster incident resolution and higher customer satisfaction. Tier 0 self-service functionality shall utilize ITO HOD's ITSM tool, integrating with other government approved tools and software as necessary.

2.2.1.4.1 IT Service Catalog

The Contactor shall develop and maintain an ITO HOD service catalog detailing the IT services offered to the DHS HQ user community. This catalog shall be created in conjunction with and agreed to by ITO HOD, describing each IT service, associated performance standards, approved hardware/software, ordering and approval processes and any other parameters dictated by the HOD. The catalog shall be configured and maintained within the ITSM tool.

2.2.1.4.2 Virtual Agent

The contractor shall design, pilot, deploy and maintain virtual agent capabilities within ITO HOD's ITSM tool. The virtual agent shall provide intelligent routing services, using scripted rules and workflows to provide automated services and user guidance. The virtual shall utilize the HOD IT Service Catalog to define services offered and allow for escalation to a live agent.

2.2.1.4.3 ITSM Self-Service Portal

The Contractor shall develop and maintain an ITSM tool self-service portal to provide Tier 0 services to the DHS HQ community. Specific capability and feature sets shall be identified through business requirement engagement workshops and maintained as new technologies/tools are deployed. Specific capabilities include, but are not limited to:

- Centralized knowledge management repository including knowledge articles and vendor tool specifications
- Portal accessibility on any device (mobile, tablet, PC)
- EUS advanced scheduling service
- Intelligent routing via virtual agent
- Frequently Asked Questions
- User specific customizations detailing outstanding ticket approvals and open tickets

The Contractor shall maintain the ITSM Self-Service portal, updating information and workflows based on routine IT environmental changes (e.g. patches, firmware upgrades, service degradations) or enterprise refresh/new technology deployments performed by other ITO divisions or project teams. These services include:

- Front End Message changes related to service outages, events or government directed messages
- Updates to Knowledge Articles KAs and Frequently Asked Questions (FAQs)
- Changes to Service Request Catalog offerings
- Maintenance of virtual agent configurations to align with HOD service catalog/KA updates

2.2.1.5 First Contact Resolution

The Contractor shall provide First Contact Resolution (FCR) for phone call incident ticket types as defined in Appendix E FCR Incident List. Service Desk Staff shall obtain Government approval of the FCR comprehensive list and implement the list as part of Transition-In with the business processes and performance metrics used to operate and manage the Service Desk.

The Contactor shall revisit and revise the FCR Incidents list to ensure optimal coverage and accuracy. The CO or COR shall review all submissions and removals. Any modifications requested by the CO or COR must be made within two business days of receipt and returned to the CO or COR for final approval.

2.2.1.6 IT Service Management Tool/Ticketing System Support

The Contractor shall provide Operations & Maintenance (O&M) administrative services in support of the HOD ITSM tool. This support includes the management of the ticketing system workflows, module interrelationships, problem and resolution categories, mappings, reporting, and interfaces in correlation with the IT Service Management Tool's best practices. The Contractor shall modify the ticketing system to accommodate any changes to process workflows or business needs. This maintenance shall follow ITSM governance processes and procedures. In addition, the contractor shall contribute to the development of requirements necessary to configure, script, customize, and program the ticketing system to support internal business needs as well as the Government's governance and oversight requirements. The ITSM Tool/Ticketing System includes:

- Support for users in the creation of new assignment groups, IT service requests, forms or field updates when new IT products, processes, or performance standards are presented
- Create and deploy reports or dashboards that allow real-time or on-demand status, including management snapshots (high level information), as well as the ability to drill down to detailed information. Examples of dashboard items include, but are not limited to, the amount of open tickets, SLA performance, and VIP tickets
- Provide user and group administrative support to include user access and permissions services
- Support with configuration changes to workflows and business rules

2.2.1.7 Knowledge Management

The Contractor shall create, review, modify, and monitor KAs required to support new services, ITSD initial troubleshooting and FCR, and Self-Help which supports the DHS HQ and Component users with resolution of common issues and tasks as it pertains to EUS.

- The Contractor shall ensure KAs are identified and created to support a seamless transition from project state to production as a part of the contractor's participation in project initiatives.
- The Contractor shall coordinate with HOD and other service offices/contractors to ensure the accuracy of TO-provided KA content for services as they relate to services provided by another service office.
- The Contractor shall participate in project initiatives and provide input into the scope of the project, ensuring required KAs are identified and created to support a seamless transition from project state to production.

- The Contractor shall ensure all KAs are updated appropriately as changes to EUS occur, including application version updates, changes to user experience, etc. KAs should be well organized, easy to find, clearly written, and concise.

2.2.1.8 Customer Training

To ensure the DHS HQ and Component end users have the information and resources they need to understand changes and new services introduced to the DHS A-LAN environment, the Contractor shall:

- Provide all end users with online familiarization training for all Contractor-managed hardware and software products. The end-user training shall include Quick Tips and clearly delineate all changes and/or new features and/or changes in functionality.
- Provide end-user familiarization training for government-provided/supported hardware and software products and services.
- Offer a range of additional training courses covering the breadth of Contractor-provided/supported products/services and access to tutorial videos.
- Support end users in the use of end-user-configurable services and settings for all provided products and services, as well as guide them in the appropriate use of the provided products and services.
- Develop, maintain, and provide training to the DHS HQ and Component users for all changes to the environment (e.g., virtual, video, user guides).

2.2.1.9 Customer Documentation

The Contractor shall:

- Provide user documentation which may take several forms, including but not limited to online help, help files, tutorials, PDF documents, and printed manuals.
- Develop and maintain online end-user documentation on DSS Contractor-provided services, including commercially available products (e.g., Microsoft Office user guide), where available from the vendor. The documentation will show how to use each function of the provided version of the product or service.
- Develop and maintain Contractor online documentation for Contractor services, such as a service catalog user's guide. All documentation will be reviewed and approved by the government prior to its availability to the end-user community.

2.2.1.10 Mission Operations Centers Surge Support (Optional)

The Contractor shall provide surge support to DHS HQ Mission Operations Centers to include, but not limited to the CISA Central, NOC OPS, HOC, SOC and NOSC. These facilities are designated as 24/7 and require the Contractor to adapt to emerging and changing support as workloads and assignments may be subject to change for various reasons with little or no advance notice. The Contractor's volume of activity may increase significantly to address emerging requirements and emergency situations. The Contractor shall have the ability, capacity, and capability to redistribute workload and re-prioritize assignments within the TO without impacting mission needs, to meet immediate need as requested by the COR or the Government Task Order Manager.

2.2.2 Sub-Task: End User Support

End User Support provides end user device operations and maintenance services to the DHS HQ and Component customers. The DHS environment is dynamic, and, as such, the Department and its Components regularly establish new sites, relocate or expand existing offices, and closes facilities. End User Support may be based at one site but provide support to other sites within that geographic area either remotely or via site visits. Each area consists of multiple sites with different business units. The Contractor shall exercise flexibility to adjust staff to fully meet changing requirements. Workload may increase significantly in situations including emergent requirements and emergency situations. The Contractor shall provide a means by which to redistribute workload that will meet these increased situations.

The current equipment quantities are for baseline purposes only and do not represent a binding number. The current hardware profile includes approximately 15,000 desktops and laptops. The total number of end users is approximately 12,500 broken down by the support tiers defined below. The ITSM tool shall define the user role. The user type quantities shall be reviewed quarterly between the COR and PM.

User Support Tier	Quantity	Hours of Support
Non-NCR User Support	0	6:00AM-6:00PM, M-F, excluding Federal Holidays
Silver (Standard NCR End User)	~12,000	6:00AM-6:00PM, M-F, excluding Federal Holidays
Gold (Standard Plus NCR End User)	100	6:00AM-6:00PM, M-F, excluding Federal Holidays
Platinum (VIP NCR User Services)	400	6:00AM-6:00PM, M-F, excluding Federal Holidays
Diamond (EVIP NCR User Services)	26	6:00AM-10:00PM, M-F, 9:00AM-5:00PM, weekends, excluding Federal Holidays

The Contractor's support shall include solutions for coverage including weekends, holidays, continuity operations, inclement weather, and government shutdown.

The Contractor shall provide end-user support operations and support for the NCR DHS HQ Field Support Locations defined in Appendix C Supported DHS HQ Sites. The Contractor, at a minimum, shall:

- Provide certified, trained, and experienced IT professionals capable of provisioning, installing, testing, troubleshooting, and configuring workstations, local and network peripheral devices, and wall-mounted projectors and smart boards—all within a diverse Windows desktop environment.
- Configure and install desktop hardware and software approved by ITO HOD.
- Receive, record, and respond to incidents and fulfillment requests via the ITSM tool.
- Test all desktop hardware once installed at a user location to ensure operability before closing the service request.
- Install and configure systems, peripherals, and devices in accordance with fulfillment requests and in compliance with applicable service levels. Peripherals are considered any items that interact with the central processing unit.
- Install, remove and/or replace network cabling between computers and wall outlets. All removed or replaced cabling shall be disposed of by the Contractor.

- Provide walk-up services for scheduled appointments supporting customers at government determined locations.

2.2.2.1 EUS Incident Management

EUS shall provide support including testing, troubleshooting, and resolving incidents for Government Furnished Equipment (GFE) workstations, laptops, tablets, cellular wireless devices, peripherals and approved networked and locally connected printers and faxes, wall-mounted projectors, smart boards, VTC end-user and conference room equipment; operating systems, drivers, all approved software applications, shared drives and other approved resources, enterprise services and external services, and interfaces to or for any of the devices currently covered and approved by DHS OCIO.

Activities include, but are not limited to: re-imaging, replacing devices, re-installing software.

The Contractor shall use standard and privileged accounts to perform configuration changes, updating and resolving tickets only after verification with the end user.

2.2.2.2 EUS Service Request Management

The Contractor shall be responsible for executing service requests, adhering to SLAs and following fulfillment processes. EUS request types include:

- Install, Move, Add, and Change (IMAC) all items, systems, services, and solutions (any requests above 10 devices shall be defined as a project)
- Distribution List Membership additions and changes necessary to maintain, upgrade, remedy, reissue, install/reinstall, inventory, document, and decommission hardware and software in accordance with written DHS HQ process and procedures
- Deliver, install, and modify end-user computing devices in a manner capable of interacting with System Center Configuration Manager (SCCM), McAfee e-Policy Server, and any configuration management solutions available for support, resolving management and security issues before deployment
- Decommission end user hardware following approved decommissioning policies and procedures
- Ensure all IT solution deployments are operational at point of delivery
- Shared Drive Access
- Burn Unencrypted CDs
- Group Mailbox Access
- Activate Broadband on Mobile Device
- Onboarding and Offboarding
- Data Retention
- Continuity Event Support
- Video Teleconference (VTC)/AV Support
- Retrieve Asset for Compromised System
- Classified Spill support
- Network Printer Maintenance
- Move MFD Printer
- Replace Network Printer
- Activate Audio in SCIF

- Install Accessibility Software
- Install Software

2.2.2.3 Security Incident Management

The Contractor shall:

- Provide End User Support for activities required as the result of data spillages, malware infection, and unauthorized access events
- Respond and report security incidents in a timely manner to the appropriate ISSO
- Respond in a timely manner to such events, and shall follow Government remedial guidance including, but not limited to, device replacement, quarantining, wiping, cleaning, removal, and any and all other actions, such as segregation, collection, and coordination of delivery to DHS IT security personnel
- Provide local hands-on support as identified by the federal Incident Response Team and shall assist with the containment and remediation of security incidents on DHS systems as directed

2.2.2.4 Asset Tracking Support

The Contractor shall support the distribution of assets to end users. The Contractor shall ensure required forms and documentation is signed by the end user and Contractor EUS staff.

The Contractor shall validate that the affected asset for all service requests and incidents is properly associated to the ITSM System ticket and address inconsistencies. When, through the verification process, it is determined that inventory assigned to the customer does not match the inventory shown in the ITSM System, the Contractor shall note all information and open an ITSM System ticket identifying those assets that differ from what is in the ITSM System. Once opened, the Contractor shall route the ticket to Asset Management for validation and resolution.

The Contractor shall comply with DHS-approved asset management, software license management, and property management policies. This may include completion of forms and documentation. The Contractor shall ensure all hardware devices have appropriate asset tags when received and prior to signoff of the Form 560 or equivalent. When the Contractor identifies an asset without an appropriate asset tag, the Contractor shall note all information and open an ITSM System ticket. Once opened, the Contractor shall route the ticket to Asset Management for remediation.

When not being used, the Contractor shall return all IT assets (equipment and peripherals) to inventory utilizing and conforming with the Government's IT Asset Management contract and its prevailing forms, workflows, and procedures.

The Contractor shall notify Asset Management within 48-hours following assets being removed from service and/or recovered.

The Contractor shall recapture, reclaim, and return all abandoned equipment to inventory.

2.2.2.5 Technology Café Support

The Contactor shall design, test, deploy and support a Technology Café IT walk-up service support center

that allows for open hour walk-in or advanced IT scheduling requests. The Contractor shall include multiple stakeholders including DHS facilities, DHS ServiceNow lead and individual manufacturer OEMs to gather requirements in designing/testing kiosks for registration/check-in solutions, displays for current customer queue status and/or schedule availability and schedule management.

2.2.2.6 National Operations Center (NOC) Support (Optional)

The Contractor shall provide 24x7x365 on-site end user support for the National Operations Center (NOC) adhering to EUS SLAs. The Contractor employees shall possess or be clearable to the TS/SCI level. The Contractor shall assist security incident handlers with the containment and remediation of security incidents on DHS systems in the NOC. The Contractor shall maintain a list of all National Operations Center A-LAN workstations and ensure that the workstations are configured and patched to required levels.

2.2.2.7 CWMD End-User Support (Optional)

The Contractor shall provide dedicated on-site end user support 6:00am to 6:00pm M-F, excluding Federal Holidays, for the Countering Weapons of Mass Destruction (CWMD) office. The contractor shall provide end user technicians, adhering to EUS SLAs and support requirements.

2.2.3 Sub-Task: Video Operations Center (VOC) Support

The Contractor shall support Video Teleconference (VTC) services with both a VTC operations center (VOC) and NCR on-site dispatch support for 200 IP connected A-LAN VTC endpoints, comprising a mixture of desktop and conference room units. VTC services include hosting conferences with multiple participants (DHS Components, other Federal Agencies, State and local homeland security partners), and voice and video collaboration with document sharing and data streaming (video, satellite feeds).

VOC support services include:

- Support to install, configure, operate, and maintain video teleconferencing and multimedia services and equipment
- Conferencing and multimedia equipment including support for bridging systems, display and projection systems, electronic whiteboards, audio systems, DVD and video recording and replay, video switching systems, control systems, and video cameras
- Assist customers with the use of video conferencing systems by providing personal instruction in the use of control interfaces and procedures
- Schedule and monitor all video teleconferencing sessions
- Maintain an inventory of video conferencing equipment owned and leased by DHS
- Maintain a DHS video conferencing contact list
- Operate VTC management platform

VTC local NCR dispatch support services include:

- Conference support (sites without dedicated onsite support) requires scheduling 24 hours in advance: No more than three (3) conferences can be supported with dispatched support simultaneously or within two (2) hours of a previous commitment.
- Ad hoc support that requires dispatch (sites without dedicated onsite support) will require four (4) hours. No more than three (3) conferences can be supported with dispatch support

simultaneously or within two (2) hours of a previous commitment.

- Break/Fix Support dispatch for sites without an onsite support will be onsite within two (2) hours. Only three (3) sites for Break/Fix can be supported simultaneously. If more than three (3) sites require onsite support at the same time, service may not be a two-hour response; it will depend on the availability of resources working at issues at the first three (3) sites before support can be available.

2.2.4 Sub-Task: Project Management & Operations Support (Optional)

The Contractor shall provide project management support to assist in the design, development, procurement, implementation, and transition to O&M of all DHS HQ projects. Project Management support staff shall be proficient in and able to employ waterfall and agile project management methodologies, frameworks, and best practices to ensure the success of DHS HQ projects. Staff shall assist DHS HQ customers with planning, requirements gathering and validation, cost development (rough order of magnitude development), market research, reporting, and change orders through the design, development, procurement, implementation, accreditation, and O&M phases of each Task order project. In addition, the Contactor shall:

- Act as project manager including establishing a project schedule and managing resources
- Develop and manage all project management artifacts, including project charter, WBS, milestone charts, RACI matrix and Risk register
- Create, manage, track, and ensure accountability for items on the project schedule for Projects, Tasks, Documentation Updates, Continuity Support, and Ongoing Efforts.
- Work with the appropriate technical personnel to ensure work instructions are created
- Ensure all end user Standard Operating Procedures (SOPs), FAQs, and training material has been developed, reviewed and disseminated (if required)
- Assist in development of plans and technical briefing materials
- Organize, attend, and participate in stakeholder meetings
- Assess project risks and issues and provide mitigations where applicable

The Contractor shall also provide operational support including financial management, knowledge management, process re-engineering, trend/metrics tracking and reporting and other mission support functions.

2.2.5 Sub-Task: IMAC Project Deployment Support

The Contractor shall be responsible for providing deployment and management support for the build-out of new facilities and/or to conduct organizational relocations, office moves, reconfigurations, IMACs above 10 devices and demolitions as well as support for technology refresh or new technology roll-out initiatives. In addition, the Contractor shall:

- Develop and present project cost estimates and level of effort details.
- Organize, attend, and participate in project stakeholder meetings
- Prepare necessary presentation materials for meetings

- Ensure all clearance and access requirements are adequately coordinated in advance
- Coordinate with other vendors/DHS entities as necessary to ensure project success
- Provide and oversee IMAC deployment resources, managing daily workloads
- Assess project risks and issues and provide mitigations where applicable
- Ensure stakeholder views are managed towards the best solution
- Work with DHS stakeholders to assess/assign project priorities
- Communicate any project issues to relevant stakeholders in a timely manner

2.2.6 Sub-Task: New DHS Employee Orientation and Onboarding Support

The contractor shall facilitate onboarding and IT training for new DHS employees (federal and contractor) providing instruction on major IT services provided by IT OPS including, but not limited to, MS Office 365, ServiceNow ticketing, MS Teams, Voice Over Internet Protocol (VoIP) phones and PIV registration. The Contractor shall provide equipment onboarding management support on-site or virtually, coordinating with DHS HQ OCIO and physical security to ensure a smooth and transparent employee onboarding process. Onboarding support includes the preparation and issuance of IT equipment and all required materials for training facilitation. All training materials will be submitted for Government approval prior to any training facilitation. Training sessions will occur on a bi-weekly basis in ninety (90) minute sessions held between 0600-1800, M-F, excluding Federal Holidays.

2.2.7 Sub-Task: Network Service Change Support (Optional)

The contractor shall perform client software testing following government prescribed testing procedures and documenting test outcomes. NSC support will be limited to executable software for desktop and laptop clients that do not require packaging. The contractor will make every effort to obtain the requested software from the resource with the assistance of the customer when necessary. NSC support includes ticket management to include performing the initial assessment of user need, validating request with the customer, checking the request against DHS Technical Reference Model (TRM), performing the initial testing procedures, and routing to the correct security or engineering teams.

2.2.8 Sub-Task: Site A Support

2.2.8.1 Management Support

The Contractor shall provide dedicated management and oversight of all services and personnel defined within Site A Support, adhering to applicable SLAs and supporting unique Site A DHS component and tenants. The Contractor shall:

- Coordinate team Continuity Support for National Level Exercises, Eagle Horizon, Table Top exercises, Component trainings and real-world events
- Serve as site project manager for new build-outs /projects, life cycle replacement, and equipment excess
- Create, manage and track items on the Site Project schedule for Projects, Tasks, Documentation Updates, Continuity Support, and Ongoing Efforts
- Coordinate with Service Desk and SMT Admin support on behalf of Site A customer

- Integrate, train and conduct workshops for Operation Centers on continuity support
    - LMS NOC, LMS NOC, OneNet, SOCs, Service Desk, Asset Management, SENS3, WidePoint, DC1 EMOC, DC2 EOC, ICCB and St. Elizabeth's NOC
- Assess, stabilize, and improve overall environment through:
    - Annual wellness reviews
    - Technology review in alignment with vendor support and recommendation
- Support exercise planning efforts specific to technical team in support of events and exercises
- Support development of Weekly Quad Charts (weekly high-level overview of the program)
- Provide updates to Weekly Activity Report (WAR)
- Create, update and maintain documentation to include SOPs and work instructions
- Provide support for the RAC and ICCB specific to the continuity site
- Assist in development of roadmaps, plans and technical briefing materials
- Evaluate and recommend improvements of onsite operational performance

2.2.8.2 End User Support

The Contactor shall provide End User Support during Normal Business Hours (0600-1800, M-F, excluding Federal Holidays) to include support for workstations, laptops, mobile devices, tablets, software, networked and locally connected peripherals, operating systems, drivers, applications, and interfaces to or for any of the devices currently covered and approved by DHS OCIO. 24x7x365 service shall be provided during exercise/actual situations (as directed and approved by the CO or COR). In addition, the services include new installation, move, add and change of all items, systems, services, and solutions, as well as additions and changes necessary to maintain, upgrade, reissue, install, and dispose of them, in accordance with DHS and Site A process and procedures. In addition, the Contactor shall:

- Support National Level Exercises, Eagle Horizon, Table Top exercises, Component trainings and real world events
- Provide EUS for the National Operations Center West (NOC-W)
    - Support during NOC relocation to include outages, connectivity issues, event driven concerns
    - Weekly exercises and trainings
    - Virtual support for AMOC
- Monthly testing of 650+ workstations/laptops, printers/plotters/digital senders/scanners - (required by OSTP/OMB Directive D-16-1 and monthly testing operating procedure)
    - Testing includes: Connectivity, application testing by opening defined mission critical applications and verifying operability, verification of systems information, testing the phone capability per seat, and resolution management on any issues.
    - Manage the system monthly testing dashboard
- Image new systems and reimage workstations when required
- Complete Service Now tickets to include Incidents, RITMs and Task while meeting SLAs
- Troubleshoot system issues, to include hardware and software
- Configure and install desktop hardware and software supported while maintaining DHS guidelines and security requirements through new build-outs and Life Cycle Replacement

- Provide operations and maintenance support for the Government's legacy desktop equipment to ensure compliance with all Government security, information assurance, asset, and change management policies and procedures while conforming to all applicable SLAs
- Replace inoperable components or parts as necessary to restore normal service operations, excluding maintenance covered under a manufacturer's warranty. All replaced and inoperative parts shall be returned to Asset Management.
- Install and configure systems, peripherals, and devices in accordance with applicable service levels. Peripherals are considered any external hardware items that interact with the desktop, laptop or tablet.
- Install, remove and/or replace network cabling between computers and wall outlets, including KVM switches and cabling
- Uninstall (e.g. "decommission") all desktop hardware and software identified as 'end of life', unserviceable or otherwise are required to be uninstalled and prepared for return to Asset Management. This includes removing memory and hard disk drives and complying with other security requirements and coordinating with the Site Security Officer (SSO) for approval to remove IT equipment that is in a Sensitive Compartmented Information Facility (SCIF).
- Provide for software version upgrades as part of the ongoing support process. This includes EUS support as needed to deploy new software versions, patches and releases, including Operating System upgrades.

2.2.8.3 System Engineering/Administration Support

The Contactor shall support resiliency efforts for disaster restoration providing system administration and engineer support for the COOP HQ Domain controller, File server (DFS), printer servers, DHCP, SCCM, Jump Box and data backup environment. The Contractor shall also:

- Support Continuity Essential Records server file structure support and management
    - Support for components and MGMT LOBs
- Perform the following server administrative services:
    - Build, install, configure, maintain, upgrade, remove and/or replace server
    - System migration support and coordination
    - Perform server backups and restores
    - Monitor server performance and support for patch management
    - Test and install patches (Microsoft, application, security, etc.) per the ICCB when required
- System hardware and software standardization and tracking
    - Tracking of equipment for managing life cycle replacement schedule (per security compliance and vendor requirements)
- Represent Site on the Headquarters IPT meetings prior to deployment for of new services or upgrades
- Support the planning, design, development, deployment, and necessary support services to provide for current and future server support needs in compliance with DHS HQ direction
- Ensure all GPO memberships reflect only those members that are approved for membership and that are still active and/or supported by an active user or device
- Maintain data center and LAN closet drawings and ensure all work areas comply with DHS security and safety requirements and industry best practices

- Assist in the integration of all as-a-service capabilities to include:
    - Beta and Gamma phase testing in coordination with DHS HQ and Microsoft Engineering team
    - The DHS HQ as a Service offerings initial deployment as well as upgrades
- Be responsible for installs, moves, adds, and changes for all servers; act as liaison for other vendors with new installs, moves, adds, changes, and life cycle replacement
- Modify and enable Active Directory accounts when required

2.2.8.4 Continuity Planning and Information System Contingency Planning Support

The Contactor shall support the development of a Continuity of Operations Plan (COOP)/Disaster Recovery Plan (DRP) in coordination with the Government that will sustain Headquarter operations in the event an emergency should render the operation centers unavailable. Support may require an alternate federally accredited site(s) or solution(s) for maintaining continuity of operations during emergencies or other situations. The Contractor shall:

- Support National Level Exercises, Eagle Horizon, Table Top exercises, Component trainings and real-world events
    - Conduct Hotwash (after action meeting), create and submit After Action Reports (AARs) supporting Exercises
- Conduct Table top exercises and Workshops
    - Facilitate Hotwash (after action meeting), create and submit After Action Reports (AARs) supporting Exercises
- Support the updating of DHS HQ OCIO Continuity Plans
    - COOP, Devolution and Reconstitution Plans
- Create new, update, and maintain Standard Operating Procedures and Work Instructions
- Integrate, train and conduct workshops for Operation Centers
    - LMS NOC, LMS NOC, OneNet, SOCs, Service Desk, Asset Management, SENS3, WidePoint, DC1 EMOC, DC2 EOC, ICCB and St. Elizabeth's NOC
- Develop and implement Continuity with ITSM tool for collaborative communication
- Create, update and maintain Continuity monthly newsletters
- Create, update and roll out of Continuity trainings
    - Continuity 101, 102, 104, 200, 203, 205
- Develop and maintain a Quality Control Plan reporting quality control metrics, gap analysis, recommendations and solutions for program quality control requirements
    - Develop OCIO cross functional layouts
    - Create risk matrix identifying gaps
    - Document and improve on lessons learned
- Develop a Project Plan detailing the proposed plan for project implementation, including but not limited to, project milestones, Life-Cycle costs, scope, schedule, risks, deliverables and quality controls
- Develop and maintain a Risk Management Plan (RMP) identifying, analyzing and evaluating program and project risks
- Conduct Devolution testing with Devolution partners
    - Required by OSTP/OMB Directive D-16-1 and testing operating checklist

- Support the association of Continuity members as well as non-Continuity members
- Support and recommend Continuity team alignment/restructure and allocation
- Create, update and maintain Continuity dashboard and SharePoint site
- Create, update and maintain all critical contact lists, lines of succession, COOP reference books, Continuity ERG play books
- Support Components Continuity Working Groups (CWG)
    - Create and manage OCIO Continuity Working Groups and Tiger teams
- Provide support for the clients Information System Contingency Plan (ISCP) testing, training and exercises (TT&E) to ensure customer systems maintain Contingency in accordance with DHS 4300A and NIST SP guidance
- Conduct the Information System Contingency Plan Coordinator (ISCPC) in executing the Information System Contingency Plan (ISCP) testing, training and exercises (TT&E) for OCIO essential systems activities (ESA)

2.2.8.5 Emergency Notification System (ENS) Support

The Contactor shall:

- Manage access to all DHS components within the DHS ENS system
- Develop, update, and train components
- Provide technical support for all components in the DHS ENS system
- Liaison between DHS ENS end users and the FEMA ENS Administrators
- Develop OCIO ENS procedures and plans for operational use based on specific requirements
- Maintain accurate data for all information within the scope of permissions
- Support ENS Continuity onboarding/offboarding within ITSM tool
- Upload and maintain personnel information into the ENS system
- Support ENS Testing/Exercises
    - Develop and maintain Fed and COR/Contractor Personnel surveys
    - Support quarterly meetings to validate OCIO division/office rosters (groups) and COR group
    - Schedule and activate accountability surveys with input from federal leadership
    - Run reports and compile survey results
- Provide support for GETS and WPS to Components

2.2.8.6 Inventory Management Support

The Contractor shall provide inventory and logistics management support to include:

- Site A Inventory Management support for both Local Property Officer (LPO) and the APO assigned by the Chief Resources Section of any hardware that is moved in any space onsite.
- Support, track and report approximately 4,465 items (A-LAN, HSDN, LAN-C and communication devices) within the Site A Inventory. Report can be provided from Site Master Database and Sunflower Asset Management System (SAMS).
- Coordinate excessing Component equipment to include excessing equipment being dispositioned from SCIFs

- Conduct physical audits of equipment to ensure equipment is aligned with the correct components and support any government directed audit efforts
- Configure, test and ship items that require immediate implementation
    - Items include, laptops, mobile phones and satellite phones
    - In coordination with meeting the OSTP/OMB Directive D-16-1 and testing operating procedure
- Provide accurate accounting of all assets within SAMS and Site-specific database
    - Updating SAMS for real time tracking, collecting and recording detailed and accurate inventory, including documentation of transfers and validation of existing inventory for each inventoried IT asset item during the resolution of an incident or fulfillment activity.
- Devolution partner coordination and testing of communication equipment
- Creating, updating, and adhering to new Standard Operating Procedures and DHS polices
- Support the distribution of assets to end users ensuring all hardware devices have appropriate asset tags when received and prior to signoff of the Form 560 or equivalent. All transfers of assets shall be performed in accordance with Asset Management policies. The Contractor shall be responsible for the completion of all associated forms and documents required by Asset Management policies.
- Ensure any software that is provisioned is properly documented in the Service Now Asset Management module
- Verify and update, if necessary, the inventory of all assets during installation, removal, and maintenance activities. All hardware assets deployed shall be properly documented, signed by the end user and technician delivering, deploying or installing the item, and submitted as part of the issue process. If a device is determined to not be properly asset tagged, notify asset management and acquire, tag, and distribute the equipment or replacement parts.

2.2.8.7 Information System Security Officer (ISSO) Support

The Contactor shall:

- Provide Trusted Agent HSDN support to DHS and FEMA
- Provide C-LAN Extension Site Annual Assessment (includes updating System Security Plan) support
    - Conduct Hotwash and create After Action Reports (AAR)
- Provide HSDN Extension Site Annual Assessment (includes updating System Security Plan) support
    - Conduct Hotwash and create After Action Reports (AAR)
- Review/Validate inventory and Visio diagrams
- Support ITSM tool tickets (hardware and software approval tickets for items impacting the site and installed in SCIFs)
- Track Authority-to-Operate (ATO) letters/dates (12 (A-LAN 3, HSDN 2, LAN-C 1, Components 6) ATO letters)
- Track and support of ISVMs
- Conduct Antivirus/Microsoft Update checks of all systems
- Conduct equipment inventory within DHS approved SCIFs (11)
- Provide quarterly inventory to I&A (approximately 2850-line items every quarter)
- Sign/Validate Entry/Exit of equipment entering/exiting DHS SCIFs (includes decommissioning of equipment) (average of 18 per month)

- Conduct monthly security walk-through of DHS SCIFs (11)
    - Provide AISSO monthly security compliance checklists of SCIFS to I&A
- Develop and update procedures in support of Incident Response, MWEOC IT Equipment/Media Policy, Guest Systems entering a SCIF, and Co-Use Agreements
- Provide Incident Response support with SSO
- Provide project support to include new build-outs and life cycle replacement
    - AVKS Life cycle replacement
    - Site building 401 new build-out support

2.2.8.8 Continuity Surge Support

The Contactor shall provide support during continuity events and/or exercises that may require surge support periodically throughout the year. This is unscheduled in most cases and will be necessary to support Homeland Security Presidential Directive (HSPD)-20 requirements. Workloads and assignments may be subject to change for various reasons with little or no advance notice. The Contractor's volume of activity may increase significantly to address emerging requirements and emergency situations. The Contractor shall have the ability, capacity, and capability to redistribute workload and re-prioritize assignments within the TO without impacting mission needs, to meet immediate need as requested by the COR or the Government Task Order Manager. The contactor may also be recommended to attend training or become certified to meet evolving Site A mission and COOP requirements. Prior approval by the COR or the Government Lead is required prior to training being authorized. Continuity surge support services may also be leveraged for specific projects dictated and authorized by the COR or the Government Task Order Manager.

2.3 Task 3: Business Transformation and Innovation Services

2.3.1 Sub-Task: Business Transformation/Innovation Solution Development

The contactor shall develop and implement solutions that drive program innovation and business transformation. The Contractor shall focus on customer identified priorities, emphasizing technology and process improvements that deliver cost efficiencies, higher customer satisfaction and increased IT service productivity. The contactor shall collaborate and engage with technology service providers to align government innovation priorities with new vendor offerings. The contractor shall work with the government for each business transformation initiative to identify measurable goals and define outcomes to include:

- Whitepapers on emerging technologies and industry management best practices
- Facilitation of ideation and brainstorm session
- Hosting new technology partner/vendor for introductory workshops
- Creating business transformation and innovation roadmaps
- Developing proposals for innovation implementation and O&M sustainment (including pricing)

2.3.2 Sub-Task: Business Transformation/Innovation Implementation Support

The contactor shall utilize the solutions identified and developed as part of Sub-Task 2.2.1 to provide support for the design, pilot and implementation of Business Transformation and Innovation Initiatives. The Contactor shall follow DHS SDLC guidelines in providing project management, development (if

applicable) and engineering support to adequately design, test, and deploy each innovation effort. Each project implementation and any associated O&M sustainment support will be funded separately.

2.3.2.1 Remote Support Enhancement (Optional)

The contractor shall provide enhanced remote support capabilities, implementing new or augmenting existing tools that increase end user work productivity through faster incident resolution and request fulfillment. Support requirements may include the development of an initial proof of concept design, pilot implementation and/or production implementation and sustainment.

2.3.2.2 Executive Dashboards & Performance Analytics (Optional)

The contractor shall design, develop and maintain a dashboard and performance analytics platform that can be augmented based on user roles, enabling real-time display of DHS HQ operations. Dashboards should be available in a mobile-ready platform to maintain situational awareness, no matter the location, and incorporate multiple data sources (SolarWinds, SCOM, HP Openview, SCCM, etc.) to create an enterprise view. This platform should allow for "drill down" capabilities that deliver environmental details as needed to enable more informed, data-driven decisions.

2.3.2.3 Single Point of Contact Services (Optional)

The Contactor shall implement an enterprise Single Point of Contact approach providing one contact for all IT related incidents and requests and utilizing a Total Contact Ownership (TCO) approach whereby a ticket is owned, tracked, and updated by SPOC until resolution. TCO resolution shall be the responsibility of the ITSD regardless of who (e.g. other contractors) tickets are routed to.

2.3.2.4 Service Desk Automation Services (Optional)

The Contractor shall provide advanced automation services, providing users the ability to immediately execute/receive services without manual intervention. This support shall require advanced scripting and integration development between the ITSM tool and other applications including, but not limited to, Active Directory, SCCM, and existing DHS as a Service offerings.

2.3.2.5 PC as a Service (Optional)

The Contractor shall perform end-to-end device lifecycle management for hardware services. The Contractor shall provide computer hardware per minimum specifications as defined by ITO HOD. All hardware offerings are subject to HOD approval, to include waivers to hardware specifications. Hardware support may include:

- Hardware Refresh - Refresh hardware devices thirty-six (36) months from the initial date of deployment. Includes the ability to request Early Technology Refresh (ETR).
- Restoration - Restore an end user's device to full operability when an incident occurs that renders hardware unstable, inoperable, or with degraded performance
- Subscription Removal - Remove services from the end user environment on receipt of request
- Sanitize and Disposal - Retain systems prior to sanitization or disposal to permit recall of data
- Loaner Pool Management - Supply and manage loaner computers
- Asset Management - Define and implement procedures for asset tracking

- Audit - Participate in audit activities to ensure accuracy of documented asset information and implement necessary corrective actions
- Storage - Ensure that facilities used for storage of hardware, software, and other associated equipment include adequate protection and security, whether Government-provided or Contractor-provided storage facilities are used

2.3.2.6 Business Process Automation (Optional)

The Contactor shall provide business process automation services, digitizing paper processes, streamlining workflows and automating procedures. The Contactor shall analyze and document as-is processes, recommend process improvements and provide an analysis of alternatives for utilizing existing or deploying new technology solutions. Upon government approval, the Contractor shall pilot, test and deploy the business process automation solution.

2.3.2.7 ITSM Tool Development Support (Optional)

The Contactor shall provide development services to implemented new or enhance existing ITSM capabilities. The Contactor shall utilize an agile approach in delivering project management, business analysis, solution architecture and development support to meet emerging ITO HOD mission priorities and needs. Project initiatives will be further defined and authorized by the COR or CO.

2.3.2.8 Project Surge Support (Optional)

The Contactor shall provide project management, engineering and/or development expertise to meet emerging ITO HOD mission priorities and needs. Project initiatives will be further defined and authorized by the COR or CO.

3 Contract Personnel

The Contractor shall:

1) Provide an array of management, technical, and support staff to fulfill the operational and mission needs at all Headquarters and Component sites.
2) Provide qualified personnel to achieve all objectives specified in this Task Order.
3) Provide management, operations, and support staff to complete the above objectives. The Contractor will use best practices emphasizing standard processes, expertise in technologies, systems, hardware and software, technical management, and structured methodologies for IT systems management and operations.
4) Provide management, operations, and support staff to improve the DHS HQ IT infrastructure while driving operational effectiveness and decreasing cost and risk to the Government.

3.1 Key Personnel

The Contractor shall:

1) Identify and provide key personnel, detailed in Table 3-1, who are responsible for meeting task order objectives and tasks.
2) The government may designate additional key personnel as required and agreed upon by the Contractor and the Government. Key personnel changes shall be established after award with a contract modification.
3) Proposed candidates require review and approval by the government prior to placing the individual into the position, including initial candidates and subsequent substitutes or replacements. The Government may at its sole discretion via the CO, direct the Contractor to remove any key personnel 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 task order. The CO will provide the Contractor with a written explanation to support any request to remove an employee.
4) Notify the government no less than 30 business days in advance of any proposed substitute or change to key personnel.
5) Dedicate key personnel to DSS 2.0 for 100% of their time and efforts.

Table 3-1 Key Personnel

Key Personnel	Security Clearance	Position Description
Deputy PM	TS/SCI	During any absence of the PM, the DPM shall have full authority to act for the Contractor on all matters relating to work performed under this TO Call. The DPM shall be able to read, write, speak and understand English. The DPM shall meet DHS security clearance requirements for up to Top Secret with Sensitive Compartmented Information access. The Contractor shall not replace the DPM without prior acknowledgement from the CO. The DPM shall be available to the COR via telephone and/or email. The DPM shall respond to a request for discussion or resolution of all performance, service, delivery, and technical inquiries or problems within two (2) hours of notification.
Operations Manager	TS/SCI	Responsible for the overall delivery of IT services and support to the DHS HQ and component customers. Ensures alignment between service desk and EUS operations teams and adherence to HOD SLAs. Coordinates with other DHS contractors to ensure EUS/ITSD awareness and appropriate training/SOPs are provided in advance of new technology deployments and operations configuration changes.

Key Personnel	Security Clearance	Position Description
Chief Architect	Suitability	Responsibilities include working collaboratively with the customer to iteratively define and solution IT operation and engineering enhancements (e.g. Tier III infrastructure engineering, critical incident management, desktop engineering, automated patch management, cloud migration strategies), develop concept of operations, roadmaps and facilitate enterprise IT strategy execution sessions.
EUS Manager	TS/SCI	Responsible for the delivery of IT EUS support to the DHS HQ and Component customers. Works closely with ITO HOD to support effective delivery of the following: maintain a stable, cost effective and secure IT environment; provide quality, timely and cost-efficient maintenance; protect and present information that facilitates the DHS HQ and Component mission; and modernize technology to meet business demands in a cost-effective manner. Includes all facets of operations for computer, network, communications, and hardware and software infrastructure technologies.
Service Desk Manager	Suitability	Responsible for the delivery of IT service desk support to the DHS HQ and Component customers. Works closely with ITO HOD to support effective delivery of the following: maintain a stable, cost effective and secure IT environment; provide quality, timely and cost-efficient maintenance; protect and present information that facilitates the DHS HQ and Component mission; and modernize technology to meet business demands in a cost-effective manner. Includes all facets of operations for computer, network, communications, and hardware and software infrastructure technologies.

3.2 Essential Personnel

All personnel supporting this Task Order shall be categorized as Essential and shall continue to provide support during Government shutdowns and other government designated events. The Contactor shall ensure continuity of service during Government shutdowns, executing the business continuity plan, as required.

3.3 Staffing Plan/Personnel

The Contractor Shall:

1) Develop and implement a staffing plan outlining the overall concept of staffing for all phases of work under this Statement of Work (SOW).
2) Address the ability to realign personnel in response to a changing or fluctuating workload.

3.3.1 Personnel Security

The Contractor Shall:

1) Support the DHS HQ suitability process and security procedures, ensuring all Contractor employees meet all security requirements.
2) Perform services per policies and procedures approved by ITO HOD and that meet the DHS regulations and guidelines, including in-processing and out-processing procedures defined by the DHS HQ.
3) Ensure all Contractor personnel requiring unescorted building admission or access to DHS IT systems and data are vetted, cleared by Personnel Security, pass the DHS HQ suitability screening requirements, receive an Entry on Duty (EOD) date from the Office of Security, and sign the required forms prior to beginning performance.
4) Ensure personnel are granted access to the DHS HQ information and systems only after favorably completing an adjudicated background investigation and/or by the DHS HQ definitions in this contract, including the requirement that all of these personnel be citizens of the United States of America.
5) Ensure all personnel obtain and wear valid DHS identification badges when working at DHS facilities.
6) Manage collection of badges for personnel leaving DSS 2.0 or at the end of the Task Order.
7) Provide personnel for assignments up to the Secret level with core staff, up to the Top Secret/Secret Compartmented Information (TS/SCI) level through additional support staff, and provide for other services at the unclassified, Sensitive Security Information (SSI) level per the DHS HQ request with all clearances in place prior to commencement of the work. A waiver may only be authorized by the COR or CO.
8) Obtain and maintain the appropriate security clearances.
9) Develop and implement an escalation procedure for notifying IT security of any personnel situations that may have an adverse effect on the DHS HQ security that is approved by the government.

4 Deliverables

The Contractor shall provide Deliverables as specified in Table 4-1. The format and content of all deliverables are subject to Government approval. Deliverables may change during the course of the contract. If a deliverable is determined to be required and is not listed below, the delivery date for that deliverable shall be established after award with a contract modification.

Table 4-1 Contract Deliverable Requirements List (CDRL)

Item	Description	Delivery Date
	Plans	

1	TO Program Management Plan (PMP)	5 Calendar Days following Transition-In
2	Transition-In Plan	10 Calendar Days from Award
3	Transition-Out Plan	30 Calendar Days following Gov't Request
4	Transition Kick-off Presentation	15 Calendar Days from Award
5	Remote Support Plan	30 Calendar Days from Award, updated as necessary
6	Quality Assurance Plan	Quarterly
7	Business Continuity Plan	45 Calendar Days from Award, updated as necessary
8	Call Surge Plan	30 Calendar Days from Award
9	New Hire Training Plan	45 Calendar Days from Award, updated semi-annually
10	Standard Operating Procedures (SOP)	As Required
11	IT Service Catalog	90 Calendar Days from award, updated quarterly
Reports		
12	Monthly Status Reports	Monthly on the 5th business day of the month
13	Integrated Master Schedule	As required with regular updates
14	Weekly Operations & Projects Status Report	Weekly
15	Performance Management Report (PMR)	Quarterly on the 5th Business Day
16	Customer Reports (up to 4 per month)	Upon COR or ACOR request
17	Monthly Call Logs	Monthly on the 5th business day of the month

4.1 Deliverable Acceptance

The COR and CO have the right to reject or require correction of any deficiencies found in the deliverables identified in Table 4-1. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per the delivery instructions. The COR will have 10 business days to review deliverables and make comments. The Contractor shall have 10 business days to make corrections and redeliver. If the COR does not provide rejection within 10 business days, the deliverable is assumed accepted.

5 Security Management

The Contractor shall comply with the information security requirements as defined in the following federal standards and DHS 4300A Sensitive Systems Handbook, DHS 4300A Sensitive Systems Policy, DHS 4300B National Security Systems Handbook, DHS 4300B National Security Systems Policy, Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information within the Information System, National Institute of Standards and Technology (NIST) Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-53, Revision 3 (updated May 1, 2010), Recommended Security Controls for Federal Information Systems, and Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules. The Contractor shall comply with these IT security requirements in managing the execution of the contract, as well as in the delivery of services to end users. For any IT Security requirements that are not explicitly cited in the applicable documents list, the language in the Performance Work Statement (PWS) shall be authoritative until superseded by updates to the documents cited.

5.1 Definitions

IT resources is defined as any hardware or software or interconnected system or subsystem of equipment, that is used to process, manage, access, or store electronic information.

DHS data is any data and information, except for limited rights data or restricted software, which is produced or specifically used in the performance of a DHS contract.

All information systems provided and/or operated under this contract and in support of this contract are federal information systems. A federal information system is defined in NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems and in 40 U.S.C., Sec. 11331, as an information system used or operated by a Federal agency, or by a contractor of a Federal agency or by another organization on behalf of a Federal agency.

Managing the successful execution of the contract includes any internal or vendor-provided systems, applications, or processes that are required to properly manage the contract, that also process DHS data, and that do not directly meet end user requirements. An example might be an internal accounting system used between the Contractor and vendors.

Delivery of services includes any asset (computer, mobile, print), any application, any computing capability (O365), any infrastructure elements provided and managed by the Contractor, and any transformative enhancements provided in direct support of end users or required in the performance of end user activities.

5.2 Security Management in Executing the Contract and in Delivery of Services

5.2.1 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.

5.2.2 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 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.

5.2.3 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 CO, 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

5.2.4 Handling of Sensitive Information

Contractor compliance with this clause, as well as the policies and procedures described below, is required.

1) 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 CO'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.

5.2.5 Sensitive Information Incident Response Requirements

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 CO in consultation with the DHS HQ or Component CIO and the DHS HQ or Component Privacy Officer.

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 reVoIP solution of sensitive information incidents.

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

1) Inspections,
2) Investigations,
3) Forensic reviews, and
4) Data analyses and processing.

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.

5.2.6 Additional PII and/or SPII Notification Requirements

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 CO. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the CO, in consultation with the DHS HQ or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the CO, in consultation with the DHS HQ or Component Privacy Officer, has determined in writing that notification is appropriate.

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:

1) A brief description of the incident;
2) A description of the types of PII and SPII involved;
3) A statement as to whether the PII or SPII was encrypted or protected by other means;
4) Steps individuals may take to protect themselves;
5) 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
6) Information identifying who individuals may contact for additional information.

5.2.7 Credit Monitoring Requirements

In the event that a sensitive information incident involves PII or SPII, the Contractor shall be required to, as directed by the CO:

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:
    a) Triple credit bureau monitoring;
    b) Daily customer service;
    c) Alerts provided to the individual for changes and fraud; and
    d) 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:

a) A dedicated telephone number to contact customer service within a fixed period;
b) Information necessary for registrants/enrollees to access credit reports and credit scores;
c) 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 the DHS HQ, as appropriate), and other key metrics;
d) Escalation of calls that cannot be handled by call center staff to call center management or the DHS HQ, as appropriate;
e) Customized FAQs, approved in writing by the CO in coordination with the DHS HQ or Component Chief Privacy Officer; and
f) Information for registrants to contact customer service representatives and fraud representatives for credit monitoring assistance.

5.2.8 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 CO following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

6 Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified.

6.1 Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

6.2 Section 508 Applicable Exceptions

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 COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

6.3 Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

7 Appendices

Appendix A. Acronyms and Abbreviations

ACD	Automatic Call Distribution
AJAX	Asynchronous JavaScript
A-LAN	Unclassified Local Area Network
ATO	Authority or Authorization to Operate
BPA	Blanket Purchase Agreement
CDRL	Contract Deliverable Requirements List
CFR	Code of Federal Regulation
CFR	Code of Federal Regulations
CIO	Chief Information Office
CIO	Chief Information Officer
CLIN	Contract Line Item Number
CM	Configuration Management
CO	Contracting Officer
CONUS	Continental United States
COOP	Continuity of Operations Plan
COR	Contracting Office Representative
COTS	Commercial Off The Shelf
DHS	Department of Homeland Security
DSS	Desktop Support Service
EIT	Electronic and Information Technology
EOD	Entry on Duty
E-QIP	Electronic Questionnaires for Investigative Processing
ET	Eastern Time
EVIP	Executive Very Important Person

FAQ	Frequently Asked Question
FAR	Federal Acquisition Register
FCR	First Contact Resolution
FIPS	Federal Information Processing Standards
FTS	Federal Telecommunications Service
GAL	Global Access Listing
GFE	Government Furnished Equipment
GOTS	Government off the shelf
HER	Hardware Exception Request
HQ	Headquarters
HOC	Headquarters Operations Center
HSPD	Homeland Security Presidential Directive
HSPD-12	Homeland Security Presidential Directive 12
IMAC	Installation, Move, Add, Change
IMS	Integrated Master Schedule
ISO	International Standards Organization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSD	Information Technology Service Desk
ITSM	Information Technology Service Management
ITO	Information Technology Services and Operations
KA	Knowledge Article
LAN	Local Area Network
NCR	National Capital Region
NIST	National Institute of Standards and Technology
NLT	No Later Than
O&M	Operations and Maintenance

OAST	Accessible Systems and Technology
OCIO	Office of the Chief Information Officer
OCONUS	Outside the Continental United States
ODC	Other Direct Costs
P. L.	Public Law
PAR	Privileged Access Request
PII	Personally Identifying Information
PL	Public Law
PM	Project Manager
PMO	Program Management Office
PMP	Project Management Plan
PMR	Program Management Report
POA&M	Plan of Action and Milestones
POC	Point of Contact
POP	Period of Performance
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
RTS	Return to Service
SCI	Sensitive Compartmentalized Information
SER	Software Exception Request
SLA	Service Level Agreement
SME	Subject Matter Expert
SOO	Statement of Objectives
SOP	Standard Operating Procedure
SOW	Statement of Work
SPOC	Single Point of Contact
TM	Technical Monitor

TMP	Transition Management Plan
TO	Task Order
TRM	Technical Reference Model
TTY	Text Telephone
U.S.	Unites States
U.S.C.	United States Code
URL	Uniform Resource Locator
VIP	Very Important Person
VOIP/VoIP	Voice Over Internet Protocol
VTC	Video Teleconference
XML	Extensible Markup Language

Appendix B: Service Level Agreements

Subtask Area	Item	Service Category	Service Level	Service Level Description	Target
Program Management	**PM-1**	Program Management	Deliverables	Ensure the deliverables are delivered on time. Measure: % of deliverables received by due date FORMULA: ∑ Deliverables submitted on or before due date / ∑ Deliverables submitted	=>95.00% of the deliverables received on time, recalculated monthly
Program Management	**PM-2**	Program Management	Service Level Agreement Reporting	Ensure SLAs including targets, formulas and exceptions are actively managed and maintained and tracked and reported to government on a monthly basis. Measure: % of SLA reports accepted by the government FORMULA: ∑ SLA reports delivered and accepted by the government / ∑ SLA reports delivered	=>95.00% of the SLAs are managed, maintained, tracked and reports on time, recalculated monthly
Program Management	**PM-3**	Program Management	Training	Ensure all personnel are trained meeting all DHS and federal government mandated training. Measure: % staff compliant with training requirements FORMULA: ∑ DSS staff compliant with DHS required training / ∑ DSS staff	=>95.00% of all personnel have met training requirements, recalculated monthly
Program Management	**PM-4**	Program Management	Transition-In & Transition-Out	Ensure transition in and out activities are executed within the criteria of a mutually agreed transition Measure: % transition activities completed according to approved transition plan FORMULA: ∑ Transition activities completed according to approved transition plan / ∑ Completed transition activities	=>95.00% of all activities and functional areas recalculated per week
Service Desk	**SD-1**	Service Desk Response	Average time to answer phone	Average length of time a customer is waiting in the hold queue before reaching a Service Desk analyst. FORMULA: Calls where Service Desk responds # of Calls Answered in =<60 seconds / total # of Calls in queue CONDITIONS: 1) Measured & Reported 24x7x365 days per year, but the SLA only	=>90% answered within 60 seconds

				applies during the period 7am – 5pm local time (ET), Monday to Friday excluding federal holidays. 2) Time starts after all menu prompts within the ACD. EXCEPTIONS: 1) Acts of God, including weather [Government will provide approval to suspend]. 2) System outages, disruptions and maintenance.	
Service Desk	**SD-2**	Service Desk Response	Average Call Abandonment (ACA)	Percent of callers who terminate calls to the Service Desk prior to the call being answered. FORMULA: Calls where Service Desk responds. # of Service Desk calls abandoned / Total # of calls CONDITIONS: 1) Measured & Reported 24x7x365 days per year, but the SLA only applies during the period 7am – 5pm local time (ET), Monday to Friday excluding federal holidays. 2) Abandoned rates do not include calls where the customer hangs up in less than 30 seconds after completing menu prompts within the ACD. EXCEPTIONS: 1) Acts of God, including weather [Government will provide approval to suspend]. 2) System outages, disruptions and maintenance.	=<3% of total calls offered
Service Desk	**SD-3**	Service Desk Response	First Call Resolution (FCR)	Percentage of customer requests resolved at the Service Desk during the customer's first contact with Service Desk. This consists of all issues captured as ServiceNow tickets that qualify for First Call Resolution (defined in Appendix E) FORMULA: Tickets where Service Desk resolved FCR. # of tickets resolved at FCR / total # of FCR tickets received by DSS Service Desk CONDITIONS: 1) Measured 24x7x365 days per year.	=>80% of Calls taken

				2) FCR defined as resolved at first contact while customer is on the call. EXCEPTIONS: 1) Acts of God, including weather [Government will provide approval to suspend]. 2) System outages, disruptions and maintenance. 3) Excludes all tickets initiated by email and RaaS self-service system. 4) Does not include tickets that are warm transfers and assigned to other contractors or service providers for resolution.	
Service Desk	**SD-4**	Service Desk Response	Aged Backlog – Tasks	Percent of Service Desk tickets opened and unresolved greater than 20 business hours. This includes all Service Request Category tickets but does not include Incidents. FORMULA: # of requests opened and unresolved => 20 business hours / total # of requests resolved by DSS Service Desk CONDITIONS: 1) SLA applies during the period 7am – 5pm local time (ET), Monday through Friday excluding federal holidays. 2) Only includes tickets assigned to DSS Service Desk. 3) Time starts when assigned to Service Desk. 4) Time stops when resolved by Service Desk. EXCEPTIONS: 1) Acts of God, including weather [Government will provide approval to suspend]. 2) System outages, disruptions and maintenance. 3) Excludes all tickets assigned to non-DSS Service providers. 4) Time ticket spends in PENDING status excluded from calculation.	=<7% of tickets opened

Service Desk	**SD-5**	Service Desk Response	Aged Backlog - Incidents	Percent (%) of Service Desk Incidents open greater than 8 business hours during the reporting period as compared to total service desk incidents opened during the month. This includes all Service Desk Incident Category tickets but does not include Service Requests tickets. FORMULA: # of incidents opened => 8 business hours / total # of opened incidents assigned to DSS Service Desk during reporting period CONDITIONS: 1) Measured 24x7x365 days per year. 2) Only includes tickets assigned to DSS Service Desk during the reporting month. 3) Time starts when assigned to Service Desk. 4) Time stops when resolved by Service Desk. EXCEPTIONS: 1) Acts of God, including weather [Government will provide approval to suspend]. 2) System outages, disruptions and maintenance. 3) Excludes all tickets assigned to non-DSS Service providers. 4) Time ticket spends in PENDING status excluded from calculation.	=<5% of tickets opened
End User Services	**EU-1**	End User Services – Standard User (NCR) and Non-NCR with On-site personnel	Timeliness of technician responding to a reported incident	Average time required to respond a service issue impacting a standard user. This includes all Service Incident Category tickets. FORMULA: Tickets where on-site personnel respond. [# of Resolved On-site Service Issues < 4 hours] / [total # Resolved On-site Service Issues] FREQUENCY: Measured Daily, Reported Monthly CONDITIONS: 1) Time starts when ticket is assigned to EUS Tech. 2) Time stops when EUS Tech or Service Desk updates ticket with Tech arrival time.	=<4 business hours 95% of the time

				3) Scheduled appointments will remain pending until scheduled time. 4) Pending items are not counted against 4-hour window. EXCEPTIONS: 1) Acts of God, including weather [Government will provide approval for suspend]. 2) Not applicable during Contingency Exercises or Events	
End User Services	**EU-2**	VIP Incident Response	Timeliness of a technician's response to a reported VIP incident	Average time required to respond to a service issue impacting a VIP user. This includes all Service Incident Category tickets. FORMULA: Tickets where on-site personnel respond. [# of resolved VIP NCR on-site Service Issues =<2 hours] / [Total # resolved VIP NCR On-Site Service Issues] FREQUENCY: Measured daily, reported monthly CONDITIONS: 1) Time starts when ticket is assigned to EUS tech. 2) Time stops when EUS tech or SD updates ticket with tech's actual arrival time. 3) Scheduled appointments will remain pending until scheduled time. 4) Pending items are not counted against threshold time. EXCEPTIONS: Acts of God, including weather [government will provide approval for suspend].	=<2 business hours 100% of the time
End User Services	**EU-3**	Standard User Incident Resolution	Return to Service: Non-VIP from receipt of request from Service Desk to resolution of service incident	Average time required to resolve a service issue impacting a Standard User. This includes all Service Incident Category tickets. FORMULA: [# of EUS incidents resolved in =<4 hours] / [Total # of standard user EUS resolved tickets] FREQUENCY: Measured daily, reported monthly CONDITIONS: 1) Time starts when EUS tech arrives desk side. 2) Total time excludes hardware replacement and when ticket is	=<4 business hours, 95% of the time

				placed in pending due to customer request (e.g. scheduled appointment). EXCEPTIONS: 1) Time starts when EUS Tech arrives desk side. 2) Total time excludes hardware replacement. EXCEPTIONS: 1) Acts of God, including weather [government will provide approval for suspend]; 2) User not available within threshold window or ticket placed in pending at user request. 3) MTTR restricted to DSS realm of responsibility [where we are in control]; 4) Ordering/availability of parts; 5) Major incident (or problem) affecting 10+ users or entire site [will notify user of master ticket]. Note: Resolution includes a work-around (e.g. map user to a different printer)	
End User Services	**EU-4**	Install, move, add change (IMAC) Standard User Hardware and Software	Time it takes a technician to perform an install, move, add, change (IMAC) – includes both hardware and software	The percentage of time technicians complete Standard User IMACs within the time specified. FORMULA: [# of standard user IMACs completed =<8 hours]/ [Total # of standard user IMACs] FREQUENCY: Measured daily, reported monthly CONDITIONS: 1) Time starts when EUS tech arrives desk side. 2) Applies only to DSS supported assets. 3) Tickets limited to 1 user per ticket. EXCEPTIONS: Acts of God, including weather [government will provide approval for suspend]; user not available within threshold window, requisite hardware/ software license is available and does not require purchasing, ticket placed in pending due to user request (e.g. scheduled appointment).	=<8 business hours, 98% of the time

End User Services	**EU-5**	VIP Incident resolution	Return to service: VIP from receipt of request from Service Desk to resolution of service incident	Average time required to resolve a service issue impacting a VIP user. This includes all Service Incident Category tickets. FORMULA: Tickets where VIP incident resolved. [# of Resolved VIP EUS service issues] < 4 hours] / [total # Resolved VIP EUS Service Issues]. FREQUENCY: Measured Daily, Reported Monthly CONDITIONS: 1) Time starts when EUS Tech arrives desk side. 2) Total time excludes hardware replacement. EXCEPTIONS: 6) Not applicable during Contingency Exercises or Events	=<4 business hours, 99% of the time
End User Services	**EU-6**	VIP Install, Move, Add, Change	Time required to Move-Add-Change or remove individual software or hardware system upon receipt of appropriate request form	Average time required to complete VIP End User Device Move-Add-Changes. FORMULA: VIP Tickets where end-user services responds. [# of VIP end-user device moves-add-changes =<4 business hours] / [Total # VIP end-user device moves-add-changes] FREQUENCY: Measured daily, reported monthly CONDITIONS: 1) Time starts when EUS tech arrives desk side. 2) Applies only to DSS supported assets. 3) Tickets limited to 1 user per ticket. EXCEPTIONS: Acts of God, including weather [government will provide approval for suspend]; user not available within threshold window or ticket placed in pending at user request, requisite hardware/software license is available and does not require purchasing.	=<4 business hours, 99% of the time

End User Services	**EU-7**	NOC Incident Resolution	Timeliness of NOC incident resolutions	Total time in minutes for a technician to return end-user to operational status. Average time required to resolve a service issue impacting a user. FORMULA: Tickets where end-user services responds. [# of Resolved NOC incidents < 60 business minutes] / [total # Opened NOC Incidents] FREQUENCY: Measured Daily, Reported Monthly CONDITIONS: 1) Does not apply to incidents not reported through DSS Service Desk 2) Time starts when assigned to NOC Tech. 3) Total time excludes hardware replacement. EXCEPTIONS: 1) Acts of God, including weather [government will provide approval for suspend]; 2) VIP user not available within threshold window or ticket placed in pending at user request; 3) Issues inaccurately assigned by non-CACI person to EUS; 4) MTTR restricted to DSS realm of responsibility [where we are in control]; 5) Ordering/availability of parts; 6) Major incident (or problem) affecting 10+ users or entire site [will notify user of master ticket]. Note: Resolution includes work-around (e.g., map user to a different printer). 7) Not applicable during Contingency Exercises or Events	<60 minutes, 98% of the time
	EVIP-1	EVIP Incident Response	Timeliness of a technician's response to a reported EVIP incident	Average time required to respond to a service issue impacting an EVIP user. This includes all Service Incident Category tickets. FORMULA: Tickets where on-site personnel respond. [# of Responses to EVIP NCR On-site Service Issues] < 2 hours / total # Responses to EVIP NCR On-site Service Issues] FREQUENCY: Measured Daily, Reported Monthly CONDITIONS:	=<2 hours, 100% of the time

				1) Time starts when ticket is assigned to EUS Tech. 2) Time stops when EUS Tech or Service Desk updates ticket with Tech's actual arrival time. EXCEPTIONS: 1) Acts of God, including weather [government will provide approval for suspend]; 2) User not available within threshold window or ticket placed in pending at user request. 3) MTTR restricted to DSS realm of responsibility [where we are in control]; 4) Ordering/availability of parts; 5) Major incident (or problem) affecting 10+ users or entire site [will notify user of master ticket]. Note: Resolution includes a work-around (e.g. map user to a different printer)	

Appendix C: DHS HQ and Customer Supported Sites

DHS HQ NCR facilities shall be maintained and updated quarterly within a government determined location. Changes to the DHS HQ site list shall be approved by the Service Management Director and COR.

Appendix D: Executive VIP (EVIP) and VIP Position List

EVIP: The following position are slotted as an EVIP.

1) Secretary (S1)
2) Deputy Secretary (S2)
3) Under Secretary for Management
4) Chief Financial Officer
5) Chief Procurement Officer
6) Chief Human Capital Officer
7) Chief Readiness Support Officer
8) Chief Security Officer
9) Chief Information Officer
10) Under Secretary, Office of Intelligence and Analysis
11) Under Secretary, Science & Technology
12) Under Secretary, Office of Strategy, Policy, and Plans
13) Director, Cybersecurity and Infrastructure Security Agency (CISA)
14) Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA)
15) Chief of Staff, Cybersecurity and Infrastructure Security Agency (CISA)
16) Executive Director, Cybersecurity and Infrastructure Security Agency (CISA)
17) Assistant Secretary, Weapons of Mass Destruction Office
18) Assistant Secretary, Office of Legislative Affairs Office
19) Assistant Secretary, Office of Partnership and Engagement
20) Assistant Secretary, Office of Public Affairs
21) Executive Director, Joint Requirements Council
22) Director, Operations Coordination
23) Chief Privacy & FOIA Officer
24) Citizenship and Immigration Services Ombudsman
25) Civil Rights & Civil Liberties Officer
26) Inspector General
27) General Counsel

EVIP-R: EVIP-R are the Executive Assistant to the EVIP.

VIP: The following position are slotted as an VIP.

1) Secretary Office
    a. Chief of Staff
    b. Executive Secretary
    c. Military Advisor
    d. SES Position(s)

2) Management Directorate
    a. Deputy
    b. Associate Deputy
    c. Chief of Staff of Deputy
    d. Deputy Chief Officer(s)
    e. Chief of Staff of Chief Officer(s)
    f. Executive Director(s)
    g. Executive Director, Office of Program Accountability and Risk Management
    h. Director, Office of Biometric Identity Management (OBIM)
    i. Director, Federal Protective Service (FPS)
    j. SES Position(s)
    k. Division Director(s)
3) Deputy Under Secretary, Science & Technology
    a. Chief of Staff
    b. Executive Director(s)
    c. SES Position(s)
    d. Division Director(s)
4) Principal Deputy Under Secretary for Office of Intelligence and Analysis
    a. Chief of Staff
    b. Executive Director(s)
    c. SES Position(s)
    d. Division Director(s)
5) Office of Strategy, Policy, and Plans
    a. Deputy Under Secretary
    b. Chief of Staff
    c. Senior Official Performing the Duties of the Under Secretary for Strategy, Policy, and Plans
    d. Assistant Secretary, Counterterrorism and Threat Prevention
    e. Assistant Secretary, Cyber, Infrastructure, Risk, and Resilience
    f. Assistant Secretary, International Affairs
    g. Assistant Secretary, Trade and Economic Security
    h. Executive Director(s)
    i. SES Position(s)
    j. Division Director(s)
6) Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA)
    a. Chief of Staff
    b. Executive Director(s)
    c. SES Position(s)
    d. Division Director(s)
7) Countering Weapons of Mass Destruction Office
    a. Principal Deputy Assistant Secretary

b. Chief of Staff
c. Chief Medical Officer
d. Executive Director(s)
e. SES Position(s)
f. Division Director(s)

8) Office of Legislative Affairs Office
   a. Deputy Assistant Secretary
   b. Deputy Assistant Secretary
   c. Chief of Staff
   d. Executive Director(s)
   e. SES Position(s)
   f. Division Director(s)
9) Office of Partnership and Engagement
   a. Deputy Assistant Secretary, Office for State and Local Law Enforcement
   b. Deputy Assistant Secretary, Intergovernmental Affairs
   c. Deputy Assistant Secretary, Private Sector Office
   d. Executive Director, Homeland Security Advisory Council
   e. Executive Director, Campaigns and Office of Academic Engagement
   f. Director, Committee Management Office
   g. Chief of Staff
   h. Executive Director(s)
   i. SES Position(s)
   j. Division Director(s)
10) Office of Public Affairs
   a. Principal Deputy Assistant Secretary, Public Affairs
   b. Deputy Assistant Secretary, Media Operations
   c. Deputy Assistant Secretary, Strategic Communications
   d. Chief of Staff
   e. Executive Director(s)
   f. SES Position(s)
   g. Division Director(s)
11) Joint Requirements Council
   a. Deputy Director
   b. Chief of Staff
   c. Executive Director(s)
   d. SES Position(s)
   e. Division Director(s)
12) Operations Coordination
   a. Deputy Director
   b. Chief of Staff
   c. Executive Director(s)

d. SES Position(s)
e. Division Director(s)

13) Office of Privacy & FOIA Officer Deputy Chief
    a. Chief of Staff
    b. Executive Director(s)
    c. SES Position(s)
    d. Division Director(s)
14) Citizenship and Immigration Services Ombudsman
    a. Deputy
    b. Chief of Staff
    c. Executive Director(s)
    d. SES Position(s)
    e. Division Director(s)
15) Office of Civil Rights & Civil Liberties
    a. Deputy Officer
    b. Chief of Staff
    c. Executive Director(s)
    d. SES Position(s)
    e. Division Director(s)
16) Office of Inspector General
    a. Deputy
    b. Chief of Staff
    c. Executive Director(s)
    d. SES Position(s)
    e. Division Director(s)
17) Principal Deputy General Counsel
    a. Chief of Staff
    b. Executive Director(s)
    c. SES Position(s)
    d. Division Director(s)

VIP-R: VIP-R are the Executive Assistant to the VIP.

VIP Approver: Individuals that are designate to add end-users to the EVIP, EVIP-R, VIP and VIP-R.

1) EVIP End-User
2) Chief of Staff
3) Designated End-User Component\Office

Appendix E: First Contact Resolution (FCR) List

1) Network Drive Mapping
2) Cisco AnyConnect - VPN issue
3) Bit Locker – Recovery
4) Account Unlock – Standard
5) Account PIV Registration
6) Account PIV Exemption
7) Account Login Issues (PIV Card)

THIS PAGE INTENTIONALLY LEFT BLANK