UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES

United States Citizenship & Immigration Services
Office of Information Technology

Technical Operations Support Services

(TOSS)

Performance Work Statement (PWS)

DRAFT VERSION

April 2024

CONTENTS

1 USCIS / EID MISSION

1.1 USCIS MISSION

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is responsible for lawful immigration to the United States. USCIS administers the nation's lawful immigration, safeguarding its integrity and promise by efficiently and adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.

The USCIS Office of Information Technology (OIT) provides information technology (IT), expertise, and the strategic vision necessary to enable USCIS to deliver effective, efficient, and secure immigration services and products. OIT leads USCIS in the design, development, delivery, and deployment of IT services and solutions that are transforming the nation's immigration system.

1.2 EID MISSION

The Enterprise Infrastructure Division (EID) mission is to provide IT infrastructure, engineering, design, testing, implementation operational support services and enterprise project management. Including telecommunications, video conferencing, enterprise call center capabilities, e-mail services, and IT computing and storage at field sites and data centers.

Inherent to the EID mission is the management of the Technical Operations Center (TOC). The TOC is the central monitoring, coordinating, remediating, and reporting authority for critical incidents, maintenance, and outages for the USCIS Enterprise Architecture. The TOC is located at the USCIS Enterprise Operations Center (EOC), Stennis Space Center, Mississippi.

2 EID / TOC OBJECTIVE AND SCOPE

2.1 EID / TOC OBJECTIVE

The Enterprise Infrastructure Division (EID) objective is to manage and provide technical operations and support services required to maintain and enhance TOC O&M capabilities. The TOC supports the USCIS Enterprise Infrastructure on a 24/7/365 basis. In this role, the TOC provides support to the USCIS Enterprise Architecture which consists of 3500+ devices and 1,000+ voice and data circuits across the United States and OCONUS locations. The TOC provides technical support to the Software-Defined Wide Area Network (SDWAN) and coordinates with DHS partners for network services. The TOC supports this objective by providing support for USCIS critical applications and infrastructure by monitoring, alerting, reporting, and restoring mission essential systems and services. The TOC works collaboratively with the Security Operations Center (SOC), Enterprise Service Desk (ESD), Critical Incident Response Team (CIRT), and across USCIS OIT divisions to include ITPM system owners and stakeholders to proactively manage, monitor, report, and restore IT services.

The TOC objective is to ensure confidentiality, integrity, and availability of USICS mission critical systems and services. The TOC routinely identifies change requirements to enhance and improve enterprise performance and operations.

The TOC focuses on proactive identification of new capabilities and tools to address and remediate emerging threats and to satisfy new requirements for improved services. In this regard, the TOC evaluates and assesses new enterprise monitoring tools, capabilities, and technologies to ensure they effectively manage the USCIS enterprise infrastructure to mitigate risks of outages and improve the user experience.

The overarching objectives are:

- Provide for proactive monitoring of enterprise health and ensure optimal network availability and performance in support of organizational productivity
- Provide for timely resolution of incidents while monitoring trends and identifying and addressing root cause of common technical problems and documenting solutions to common problems before they become trends
- Ensure accurate discovery, assessment, and documentation of the operational baseline coupled with accurate and timely performance reporting
- Continuously evolve and improve monitoring techniques by implementing industry best practices, new tools, and innovative methods to include Artificial Intelligence for IT Operations (AIOps)

In meeting the objectives of this PWS, the Contractor will be expected to collaborate with OIT divisions, multiple business offices within USCIS, and external partners to conduct the work. Furthermore, the Contractor will be exposed to various USCIS IT programs and business initiatives and will be expected to cooperate and interact with multiple contractor groups supporting other aspects of USCIS IT operations. The contractor must provide seamless cooperation and productive interaction among all involved parties. Professional and productive collaboration among all supporting groups is of paramount importance to USCIS OIT senior management.

2.2 EID / TOC SCOPE

The scope of this PWS includes the following functions:

- Enterprise Monitoring (CONUS/OCONUS)
    - USCIS Networks
    - Systems
    - Applications
    - Services
- Critical Incident Management
    - Incident Reporting
    - Incident Escalations
    - Incident Resolution
    - Root Cause Analysis
- Engineering, Infrastructure, and Implementation Support
- Operations and Maintenance Support
- Policy Input
- Program and Project Management
- Dashboard Management and Reporting
- End-to-End Performance Monitoring and Alerting
- Customer Service
- Performance and capacity assessment, monitoring, and planning
- Develop and implement Automation and Orchestration

- Develop and implement Artificial Intelligence for IT Operations (AIOps) capabilities
- Adhoc Executive Reporting
    - Develop and Send Executive Notices
- Coordination with Application Teams, ITPM's and Development Teams
- Conduct Executive and Business Briefings
- Collaborate with DHS and Components to meet agency requirements
    - Inbound / Outbound networks at EQA/EQS to Cloud Services
- Manage CIRT Bridge calls
- Support SDWAN migrations
- Support USCIS change / configuration management and change deconfliction
- Provide DevSecOps to develop and create new capabilities to support operational objectives
- Manage emergency notifications in support of service incidents along with staff safety and accountability

Implementation of this scope will require the contractor to utilize multiple commercial off-the-shelf (COTS) software tools and programs, which will likely change and evolve throughout the duration of the contract. USCIS reserves the right to change the strategic direction of the technical implementation of the Task Order. This includes adapting to new and/or evolving technical approaches, as well as providing technical and program support to research, consult, and implement emerging technologies that the USCIS Chief Information Officer (CIO) deems appropriate to support the Agency's goals, objectives, and strategic vision. USCIS requires the ability to respond to emerging technology and trends that may benefit the customer. Trends may include, but are not limited to, technologies such as robotic process automation (RPA), Artificial Intelligence (AI), and Machine Learning (ML). Surge capability shall be required to provide to assess and implement technological advances as they arise to include integrating technologies into the Agency's landscape, as necessary. War rooms, tiger teams and specialized working groups may be stood-up to address and resolve critical issues and to discover, create, upgrade, and migrate these technologies. Reports, diagrams, and white papers produced during these meetings are considered government property and may be incorporated into the Technical Operations Center Playbook, a knowledge management article (KM) and/or USCIS' Information Technology Service Management (ITSM) tool at the government's discretion. Such shifts in the technical approach are within the scope of this Task Order.

3 CURRENT STATE

3.1 TOC OPERATIONS

The Enterprise Infrastructure Division (EID) currently receives Technical Operations Support Service under the existing TOSS support contract ending in FY25.

The TOC handles approximately 14,000 incident tickets annually. The TOC generates its own tickets based on notifications from alerts obtained from monitoring efforts or from other internal and external sources.

There are three different types of incident tickets which will require troubleshooting response.

Tier Level Task Areas:

- Tier I – Configuration Management, Data Collection, Troubleshooting, Implementation, Network Mapping, Network and Application Monitoring

- Tier II – Configuration Management, Data Collection, Data Integrity, Troubleshooting, Implementation, Network Mapping, WAN Monitoring, Escalation Process and Coordination
- Tier III – Configuration Management, Data Collection, Troubleshooting, Fault Monitoring, Performance Monitoring, Capacity Monitoring, Maintaining Baseline, WAN and LAN Monitoring, Security Monitoring, Analysis Reporting and Coordination

USCIS has a formal Configuration Change and Release Management (CCRM) process for the conduct of Change Requests. The process involves the submission of requests through the ServiceNow incident and Problem Management Tool. Requests are tracked through completion and the TOC will be responsible to keep the system updated on those changes that are assigned to them. There were approximately 455 Work Orders for the last 12-months. The number of incidents in the last 12-months was approximately 14,182, and the number of Change Requests (CRs) were 674. In addition, the TOC team participated in approximately 74 Critical Incident Response Team (CIRT) Bridge calls with a total of 2,015 calls during the last 12-month period which includes but not limited to maintenance calls, technical bridges, and daily calls. The time a Work Order, Incident or CR will remain open is variable dependent upon the resources, wait times and other variables. USCIS has calculated the following averages: The average open time for a Work Order was 24 hours for the last 12-months. The average open time for an Incident was 17.6 days and the average open time for a CR was 152.75 days for the last 12-months.

3.2 TOC TOOLS AND DEVICES

Appendix A contains information about the current devices used on the network. Appendix B provides a list of tools used to deliver monitoring and security capabilities.

4 TASKS

The contractor shall execute the requirements of this PWS through the following tasks.

4.1 TASK 1 - TRANSITION IN

The contractor shall be responsible for the transition-in of all technical activities by task area. To enable transition in, the Contractor shall develop a Preliminary Transition Plan as part of their proposal and submit Final Transition Plan within 15-days after notice-to-proceed.

The transition period shall not exceed 120 days.

The Transition Plan must include how the contractor will:

- Coordinate and transfer knowledge between the new and incumbent contractors
- Orient and train new contractor staff
- Assure no disruption of operations
- Learn and assume operations of TOC toolsets currently in use
- Provide a detailed Work Breakdown Structure (WBS) that shows time-phased transition milestones and a clear roadmap to full operations
- EOD status of new contractor staff

- Obtain privileged user accounts necessary for job duties

The Contractor shall develop a Transition Communications Plan to include:

- Transition team directory and organization chart
- Schedule for weekly transition meetings
- Proposed template and schedule for delivery of status reports
- Escalation sequence for government questions or issues
- Hiring status and EOD suitability of all TOC personnel
- Transition risk and planned mitigation
- Draft schedule and identification of support by Tier
- Privileged user account status of the team

Upon completion of performance of this Task Order, the contractor shall fully support the transition of work that is turned over to another entity, either government or a successor contractor, and shall be in accordance with Federal Acquisition Regulation (FAR) 52.237-3. The details of Transition-out will be outlined at the time required.

4.2 TASK 2 – ENTERPRISE MANAGEMENT

4.2.1 ENTERPRISE MANAGEMENT

Enterprise Management includes Configuration Management and Backup, Data Collection, Data Integrity, Troubleshooting, Implementation, Creating and Updating Network Mapping, Verification of Hardware and Software Licenses and Maintenance Agreements to enable the dispatching of vendor support. The contractor shall utilize log metric data as a part of the troubleshooting and proactive monitoring and alerting of the USICS Enterprise Architecture. The contractor shall proactively monitor, support, and maintain the enterprise infrastructure. The contractor shall proactively monitor end to end performance and support USCIS cloud applications and infrastructure; further, the contractor shall maintain accurate mapping of interconnections of USCIS applications and infrastructure, and Configuration Management

The contractor shall be responsible for configuration management using current O&M tools suite; ServiceNow, SolarWinds, New Relic or similar products which USCIS might procure and incorporate in the future. The contractor shall manage the configuration of all TOC managed devices. For a list of devices, refer to Appendix A. Examples of configuration management of this type are:

- Hardware and virtual device configurations to support end systems
- Monitoring configurations (i.e. Simple Network Management Protocol (SNMP) and logging configurations for integration)
- Logging daily operations (or similarly purposed solution)

The contractor shall perform the following activities:

- Support Change Requests originated by CCRM and systems

- Process received alerts from monitoring tools such as Cisco DNAC, SolarWinds, Splunk and New Relic on configuration changes made on the network devices and map the alerts to an incident ticket or a change request
- Use USCIS tools to backup configuration for USCIS systems. The contractor shall ensure that the backup is protected from unauthorized access and in control of USCIS.

The Contractor shall generate a daily Unauthorized Change Report and forward it to Enterprise Operations Center management. The report shall consist of the type of change, configuration made, time of change, username, and device name.

4.2.2 DATA COLLECTION

The Contractor shall develop and maintain TOC relevant dashboards as needed and are responsible to:

- Collect data from hardware and virtual devices, document and provide analysis in support of ServiceNow tickets.
- Collect data on incidents. Accurate incident descriptions, work performed, and data collected to identify root causes that ultimately reduce the number of tickets and prevent reoccurring incidents. It is an important function of the contractor to supply data to open tickets, process tickets, and resolve tickets in ServiceNow and as required by other agencies and vendors. The contractor shall proactively monitor the enterprise application and user performance to identify and remediate potential issues before they present negative impact (See Appendix B). The contractor shall be responsible to accurately:

    - Describe the issue
    - Describe the stakeholders involved with the ticket
    - Provide relevant data for escalation to support the ticket [Critical Incident Response Team (CIRT) / Critical Security Incident Response Team (CSIRT) transfer group]
    - Describe actions performed during the ticket investigation (to include when no action is taken)
    - Provide actions performed to resolve ticket (if applicable)
    - Describe the root cause of problem (if applicable and if known)
    - Provide sufficient detail so that another person could continue to work on the ticket, or understand all actions that occurred during the ticket process without any previous knowledge of the ticket issue
    - Provide clear and traceable representation of all work performed by the USCIS TOC

- Collect data on system availability and up-time metrics using available tools. System, network, application, and services availability both planned and unplanned down-time information shall be collected and reported on monthly basis and accumulated annually. Statistics shall be maintained and made available in raw, graphical, and statistical formats with explanatory narratives. Data Collection requires cross-functional coordination to include and is not limited to government and contractors (other contracts).

- Data collection may require representation from the contractor in war rooms, on tiger teams and specialized working groups at the government's discretion.

    Data Collection and Integrity - The contractor shall compile and manage discrepancy reports to maintain data integrity. This work is a Tier 2 level task. Discrepancy Reports (DRs) at a minimum include:

    - Operational devices not reporting data or misinformation
    - Enterprise management services incorrectly analyzing data

- Identification of lost or misinterpreted data
- Time or data gaps identified in a ticket
- Misinterpretation of data or misrepresentation of data
- Poor process or lack of process defined for ticket category
- Poor coordination process or lack of process with ticket stakeholders

4.2.3 TROUBLESHOOTING

The Contractor shall troubleshoot issues recorded in Service Desk tickets assigned to the TOC. Troubleshooting activities include, but are not limited, to the following:

- Verify the ticket and define the scope of the issue
- Gather information regarding the issue
- Utilize the appropriate Knowledge Management Article (KMA) or Knowledge Base (KB)
- Resolve problems within the scope of the USCIS TOC responsibilities
- Manage coordination and/or escalation procedures throughout the lifecycle of the ticket, or until ownership is transferred to the CIRT, CSIRT, or Emergency Operations Center (EOC). (As noted above, escalation of the ticket to the CIRT or CSIRT may not end the TOC's involvement in resolution of the issue)
- Provide ongoing reporting to management in the event of critical issues in accordance with the documented Incident Management procedures published in Knowledge Management and the USCIS TOC Playbook (a subset of the Knowledge Management)
- Provide troubleshooting data as requested by the government to remediate and close incident ticket

4.2.4 IMPLEMENTATION & MAINTENANCE

As part of its enterprise infrastructure maintenance, USCIS requires the installation, upgrade, or replacement of applications, tools, devices, switches, routers, firewalls, load balancers, and other devices. The notional process below is provided for work planning purposes. The full procedures are available in the Knowledge Management module of ServiceNow, to which the Contractor will get access upon award.

For replacement of applications, tools, network devices, switches, routers, etc. the contractor shall:

- Initiate contact and coordinate with the vendor, carrier, or appropriate agency to arrange for the delivery of the device to anywhere within the USCIS enterprise.
- Initiate contact and coordinate with the USCIS Engineering team or the USCIS Enterprise Service Desk team who will configure and install the device.
- Verify that the device was appropriately configured and is fully operational.

For installation of new applications, tools, network devices, switches, routers etc., the contractor shall:

Receive the Work Order and/or Task through ServiceNow. This ensures that the TOC is aware that the new device is being added. After the installation, the contractor will verify that the device was appropriately configured and is fully operational. The goal is to provide smooth transitions from the existing to the new network devices. In the event a service has not been properly implemented, the contractor shall provide a Discrepancy Report (DRs) to the EOC federal manager describing the problem and recommendations for resolution to further improve the process, if appropriate. For upgrade of applications, tools, network devices, switches, routers, etc. the contractor shall:

- Submit work orders through SNOW, coordinate with site personnel, schedule maintenance window, publish schedule, perform upgrade, ensure restoration of services, and follow-up with site personnel as needed.

Although the Contractor is not liable for the work of the third party, the Contractor will be accountable for all metrics, initiation of action, escalation, follow-up, etc., which are associated with this task and will be expected to remain engaged from initiation of the work through satisfactory completion to include (as requested by the government) ticket closeout and reporting.

4.2.5 PERFORMANCE AND CAPACITY PLANNING

Application and Network Performance support includes the dual function of maintaining the performance tools which are used within USCIS as well as using the tools for troubleshooting application and network performance issues. The contractor shall perform patching, and ensure configurations are backed up to keep these devices operational per best practices. Document procedures and update Standard Operating Procedures.

This task area consists of providing continuous improvement, management, maintenance, redesigns, scaling, and modernization of the USCIS performance and capacity planning and monitoring tools.

Performance optimization is of high importance due to the shared nature of these resources. The contractor shall use and configure monitoring tools and perform real time tracking of resource utilization with a focus on forecasting trends and developing proactive solutions.

The Contractor shall perform the following:

- Performance and capacity planning for enterprise performance monitoring solutions prior to implementation
- Analysis of end-to-end performance impacts and costs associated both monetarily and operationally
- Capacity analysis, bandwidth studies and risk-analysis reports should be delivered prior to the delivery of any solution, to not negatively impact the enterprise LAN/WAN and Cloud Interconnects
- Achieve maximum network performance for the enterprise users on both wired and wireless, as well as for remote teleworkers
- Produce repeatable reports that evaluate capacity and identify areas where improvements can be implemented
- Analyze specifications and capacity and undertake appropriate calculations to estimate resource requirements, in terms of labor, tools and materials
- Create capacity plans that meet Government defined business targets and optimize efficiency and costs
- Evaluate solution requirements and deliver minimum and maximum performance metrics to set thresholds; forecast when under or over conditions exist; provide mitigation/corrective action strategy
- Identify and document potential pitfalls, issues, challenges, and potential resolution strategies
- Provide continuous review of software and hardware solutions so that the organization can better anticipate customer needs
- Provide application performance analysis and reporting both as regularly scheduled and on demand
- Provide O&M support for government provided performance tools to include (but not limited to) Aternity, SolarWinds, and New Relic
- Provide Oracle Enterprise Manager (OEM) application metrics reporting, as needed to provide ad hoc reports and analysis

- Provide technical review of application performance analysis provided by USCIS, and/or other USCIS contractors or stakeholders and provide recommendations for improvement
- Assemble, lead, or participate in cross functional teams to analyze complex system problems using available tools. Team membership may span all available technical support
- Provide reports for system CPU, memory, disk utilization and capacity on a scheduled and ad hoc basis
- Coordinate efforts between application development and operation teams to meet performance standards
- Provide concise recommendations to the development and operation teams along with other stakeholders
- Provide ServiceNow workflow, automation development and support
- Develop and support Business Analytic Dashboards
- Create views and/or dashboards that will provide application performance metrics to various stakeholders
- Configure, establish, and utilize SNMP and NetFlow data within SolarWinds and additional products to provide performance metrics for workstations, servers, and network equipment
- Provide O&M support to the USCIS network tools including, but not limited to, SolarWinds, New Relic, Cisco DNA, Cisco ISE, Aternity, Ansible, Ansible tower, and Jenkins
- Create SolarWinds reports for Wide Area Network (WAN) performance on a scheduled or ad-hoc reporting basis as a part of establishing enhanced automation
- Diagnose and resolve application deployment and system problems for multi-tier systems. These web-based systems include both JAVA and .NET environments
- Support for Platform Engineering and DevOps Integration
- Create a tools analysis report and provide the government with recommendations on cost savings
- Provide application performance monitoring to include New Relic APM, Synthetics, Insight and Infrastructure

4.2.6 AUTOMATION AND ORCHESTRATION

The contractor shall continuously implement automation and orchestration to develop processes and procedures to further reduce the resource constraints, reduce human error and project backlog, and achieve optimal support for stakeholders. Additionally, where work could be turned into a task rather than a project, the “one touch to many deliverables” should be embraced where applicable.

The Contractor shall perform the following:

- Automation of new site deployments via orchestration
- Development of tools to instrument internal support and operational processes
- Increase infrastructure and software delivery speed to customers
- Achieve compliance in a faster, easier, and less expensive manner
- Compliance checking and reporting of template baselines
- Forced configuration through compliance remediation
- Dashboard creation for visibility into the USCIS WAN, LAN, Security, Wireless, UC, Hyper Converged Infrastructure, Server Platforms and alike
- Implement automation procedures for protocols, requests and changes for record keeping, to aid users, administrators, and security
- Develop an intuitive policy-based routing solution using automation and orchestration
- Utilize USCIS ticket and incident management system for automated delivery

4.2.7 NETWORK OPERATIONS

The contractor shall provide Network Subject Matter Expertise in support of all aspects of the USCIS Network Infrastructure Operation. Network Infrastructure includes SD-WAN overlays, routers, switches, Load Balancers, Firewalls, Wireless Access Points, ISE, Wireless concentrators, IDS/IPS devices, and VM's.

The Contractor shall perform the following:

- Provide recommendations on changes required in the environment, on the network, or to any device/service within the infrastructure; and upon government approval, execute the change
- Support and maintenance of the network infrastructure tools to ensure correct operation within the USCIS network infrastructure as directed by USCIS OIT Management
- Review and consult on network designs provided by the USCIS Network Engineering and Architecture, other USCIS contractors or stakeholders
- Review and provide recommendations to government managers for USCIS, DHS and ATT/Acuative Change requests that are reviewed at the Change Request Boards (CRB)
- Work with vendor's technical support personnel to perform technical analysis, troubleshooting to resolution, provide reports, and user training - document and report all findings to USCIS OIT
- Analyze tools currently in use and provide the government with recommendations on cost savings
- Provide network assistance and expert advice in the resolution of incidents elevated to the Critical Incident Response Team (CIRT). The CIRT is responsible to contact and triage the appropriate experts to collectively solve technical issues across the USCIS infrastructure and its applications. Once contacted by the CIRT, the contractor will remain engaged until the issue is declared resolved or the contractor is released by the CIRT
- Monitor the assigned queue(s) for incidents, provide expert analysis to resolve problems, record the resolution into the USCIS ticketing system, de-brief on troubleshooting outcomes and provide lessons learned via after-action reports (AAR's), incident analysis reports (IAR's), or knowledge base (KB) articles.
- Provide support for Cloud routers and other network equipment in Equinix, AWS and Azure to include but not limited to ASR, Security groups, VPCs, and VPGs.
- Assist Engineering and Architecture team in the rollout of new products and services on the network as needed to include, but not limited to, IP address assignment, VLAN assessments, switching/routing connectivity and troubleshooting as necessary.

4.2.8 NETWORK MAPPING

USCIS currently has approximately 400 network maps stored in its EIDOCS website. The contractor shall routinely review and verify the accuracy of (USCIS operational network and attached assets) and request updates to network diagrams as needed. An accurate and timely network map aids significantly in troubleshooting, proactive efforts, auditing, and baseline network activities. Some tools available for discovery (Reference Appendix A).

4.3 TASK 3 – ARTIFICIAL INTELLIGENCE OPERATIONS (AIOPS)

4.3.1 DEFINITIONS

- AIOps: Artificial Intelligence for IT Operations, using Artificial Intelligence techniques such as Machine Learning (ML) and Natural Language Processing (NLP) to maintain IT infrastructure efficiently.
- Domain-Centric AIOps: AI intervention for a single domain within an agency, focusing on a specific purpose.
- Domain-Agnostic AIOps: AI intervention providing a holistic view of the enterprise, using data from various sources.

4.3.2 TECHNICAL NEED

USCIS requires a contractor to provide AIOps services to enhance the efficiency, proactiveness, development, and insight into the day-to-day mission to provide O&M and Sustainment support to the USCIS Enterprise. The Contractor shall:

- Implement an AIOps platform within the USCIS Technical Operations Center.
- Provide both Domain-Centric and Domain-Agnostic AIOps as applicable.
- Improve Key Performance Indicators
    - Increase Mean Time Between Failures (MTBF)
    - Decrease Mean Time to Detect MTTD)
    - Decrease Mean Time to Investigate (MTTI)
    - Decrease Mean Time to Resolve (MTTR)
- Data consolidation from multiple toolsets and sources to help aggregate

4.3.3 SPECIFIC REQUIREMENTS

- Preform an assessment of current USCIS agency authorized tools / platform and AIOps capabilities. The contractor shall have ability to research, consult, and implement emerging technologies.
- AIOps Platform Implementation: implement an AIOps platform to establish automated IT functions to enhance and improve system performance.
- Predictive Analytics Implementation: Implementing predictive models to forecast potential issues. Performance and analysis of increasing volume of data by applying AIOps techniques to predict and prevent problems.
- Root Cause Analysis: Providing tools to perform detailed root cause analysis.
- Anomaly Detection: Events and activities in datasets that suggest a potential problem.
- Event Correlation: Group events off similarities and consolidate alerts for investigations.
- Automation: Reports and Insights, routine tasks and collect data from multiple sources to help troubleshoot and remediate incidents.
- IT Service Management (ITSM): Define system thresholds and automate response ITSM Frame managing service offerings.

4.4 TASK 4 - ENTERPRISE OPERATIONS MONITORING

The Contractor shall provide 24/7/356 end-to-end monitoring of USCIS network and application infrastructure, including servers, storage, security, network devices, and services across the USCIS enterprise infrastructure at all USCIS sites including services and infrastructure within DCAP1, DCAP2, and multi-cloud hosted environments (AWS and Azure). This will be accomplished with the current approved USCIS monitoring suite of tools. Upon incident notification or alert, TOC troubleshooting shall be provided making maximum use of the available tools in accordance with Knowledge Management (KM) documents. Escalation shall also be done in accordance with KM documents. The contractor shall be responsible for maintaining and updating KMs as environmental, infrastructure, and/or process changes occur. The contractor shall have expertise with the entire suite of network and application monitoring tools used to monitor and alert on USCIS networks and applications.

4.4.1 FAULT MONITORING (DETECTION, ISOLATION, RECOVERY)

The contractor shall be responsible for fault monitoring of all operational devices, applications, and services on the USCIS network, as identified in Appendix A. Fault monitoring detects, identifies the instance, and alerts / reports when a component of a USCIS service experiences a problem. Fault monitoring determines if the service is degraded or unavailable. Upon discovery of a fault, the contractor initiates a ticket and follows the appropriate procedures as outlined in the KM.

4.4.2 PERFORMANCE MONITORING

The contractor shall be responsible for end-to-end performance monitoring of operational USCIS services, as identified in Appendix C. The end-to-end infrastructure is defined as all services and devices, both physical and virtual, which comprise the USCIS Enterprise IT infrastructure. The contractor shall use all available enterprise monitoring tools to include but not limited to USCIS systems (reference examples in Appendix A). The number of alerts per day for these systems is expected to be in the range of 500 to 1000, based on operational impact. Response to these alerts shall be in accordance with KM document instructions. The Contractor shall escalate and notify the scheduled on-call staff (technician) to assure the appropriate resources respond and address the incident. The KM document for the Mission Essential Systems (MES) alerts provided by the system owner includes but are not limited to instructions on where the event incident ticket is to be assigned based on the nature of the problem. The contractor shall assess and analyze alerts and incident information and make recommendations if thresholds need to be modified to meet performance goals and expectations.

The contractor shall use any/all USCIS provided tools to diagnose performance problems. Support shall include determining performance problems impacting USCIS Applications, services, and network infrastructure. USCIS applications consist of both on-prem hosted applications and multi-cloud environment hosting. Performance monitoring identifies important characteristics of each service component and reports if data reaches a threshold for that characteristic. Performance monitoring determines the health of the service and ensures a satisfactory end-user experience. The contractor shall be responsible for monitoring service performance utilizing the enterprise performance monitoring tools. The contractor shall review alerting thresholds to ensure performance and experience goals are being reached and strive to eliminate “false positive” alerts.

4.4.3 CAPACITY MONITORING

The contractor shall be responsible for monitoring the capacity of all operational USCIS services, as identified in Appendix B. Capacity monitoring identifies important capacity characteristics of USCIS applications, services, and Network Infrastructure and reports if data exceeds a specific threshold for that characteristic. Capacity monitoring

determines if the service must scale to meet demand for the service. The Contractor shall develop and maintain a USCIS Capacity Management Plan. The contractor shall monitor service capacity using enterprise capacity monitoring tools. Upon discovery of a capacity alert, the contractor initiates a ticket and follows the appropriate procedures as outlined in the KM.

4.4.4 FAULT, PERFORMANCE, AND CAPACITY OPERATIONAL BASELINE MANAGEMENT

The contractor shall collaborate with USCIS Delivery Teams to assess services and develop and maintain a Standard Operating Procedure for the operational baseline for USCIS applications, services, and infrastructure. The operational baseline is a composite of fault, performance, and capacity monitoring for all USCIS IT services, as referenced in Appendix B. Services shall be considered any application, system, infrastructure, or process component that supports the documented mission of the TOC as captured in Standard Operating Procedures.

4.4.5 MONITORING USCIS APPLICATIONS, SERVICES, AND NETWORK INFRASTRUCTURE

The Contractor shall provide Subject Matter Expertise (SME) to monitor USCIS Applications, services, and network infrastructure.

The contractor shall provide SME to monitor the LAN to include servers, storage, and tape backup units at the USCIS locations. Upon discovery of a capacity alert, the contractor initiates a ticket and follows the appropriate procedures as outlined in the KM.

The contractor shall provide SME in monitoring the WAN to include circuits, routers, virtual gateways, AT&T EIS vendor managed routers and DHS NOSC managed routers. The contractor shall work with DHS NOSC and vendor managed routers to ensure the devices are being monitored and receiving alerts.

The contractor shall provide SME in monitoring firewalls and the security appliances listed in Appendix C. The contractor shall work with the SOC to make sure the devices are being monitored and receiving alerts. The contractor shall maintain a list of devices monitored and provide USCIS a monthly report on the alerts reported and action taken and with Adhoc reports when requested by the Government. The contractor shall monitor configuration changes on firewalls utilizing Algosec and appropriately respond per guidance of applicable KMs for change management.

The Contractor shall monitor and report on the status of enterprise backup services which are accomplished through Veeam, SolarWinds, and Veritas NetBackup. All data center backups are scheduled through NetBackup. Enterprise backups include Service Centers and other field sites that backup data to disk or to tape.

For any jobs that fail, the contractor shall:

- Report to the government operation managers, via email, any jobs that did not complete successfully. This report will include percent of jobs successful and percent of jobs failing
- Escalate to technical staff per the KM, any failed backup jobs
- Provide preliminary analysis of the failure, and if correctable per the KM, restart or reschedule any failed job. Actions taken will be reported in the daily backup report
- Update changes to the backup jobs in the daily report. Changes may occur as the result of enterprise sites being added, as data center backups are modified for new applications or other reasons. The contractor

shall work with the backup technical staff responsible for engineering, set up, and management of the backup services, as indicated in the KM

The contractor shall respond to notifications from all DHS components, DCAP1, DCAP2 (Equinix Data Centers), and all USCIS operational locations (fixed sites, forward deployed, and embedded personnel locations) to include CONUS and OCONUS and follow the procedures in the KM to resolve. The contractor shall also respond to other Outside Government Agencies (OGA) and business partners such as, but not limited to, JP Morgan Chase and the Social Security Administration, AAMVA, HHS/CMS, DOJ, etc...

4.5 TASK 5 – INCIDENT RESPONSE AND ANALYSIS

The contractor shall manage, respond to, report on, and properly process (resolve or escalate as required) all incidents reported to the TOC. Incidents include all requests, work orders, changes, and or projects that govern the activity required to support the USCIS enterprise. Examples would include issues impacting switches, routers, firewalls, servers, riverbeds, load balancers, and applications or services supporting the USCIS enterprise. The contractor shall follow the procedures established in the USCIS Incident Management (IM) Process. The contractor shall be responsible to assist the government in keeping the IM Process current when necessary.

There were approximately 3,415 Work Orders for the last 12-months. The number of incidents in the last 12-months was approximately 1,185 and the average number of Change Requests (CRs) was 50. In addition, the TOC team participated in approximately 430 Critical Incident Response Team (CIRT) Bridge calls in the last 12-months. The time a Work Order, Incident or CR will remain open is variable dependent upon the resources, wait times and other variables. However, for the top ten types of issues, within each category, USCIS has calculated the following averages: The average open time for a Work Order was 3.57 days for the last 12-months. The average open time for an Incident was 4.11 days and the average open time for a CR was 37.87 days for the last 12-months.

4.5.1 ESCALATION PROCESS

The contractor shall be responsible for identifying and documenting escalation procedures and implementing those procedures with each group with which it must coordinate to provide event remediation. Many USCIS Services require multiple groups to solve an issue. The TOC coordinates with these groups by using defined escalation processes. All processes, procedures, points of contact, and the knowledge management articles shall be maintained in ServiceNow. The goal of defining, documenting, and implementing consistent escalation processes for each group is:

- To reduce incident and outage impact by having points of contact and processes in place during event remediation
- To consistently inform government group representatives and government service line owners of event remediation coordination efforts
- To continuously tune escalation processes to receive superior event resolution results

For escalation processes that do not produce desired results the contractor shall produce an After-Action Review (AAR) that describes the undesirable results and possible recommendations to improve the escalation process.

4.5.2 TOC CRITICAL INCIDENT MANAGEMENT

The contractor shall develop processes and tools to manage critical incidents that impact multiple users, critical sites, and critical business applications, services, and infrastructure. The TOC Critical Incident Management process is *not* intended to address individual user issues that are normally handled by the Service Desk / CIRT team. The TOC Critical Incident Management process should define what steps are required to handle various outages to assist in incident resolution / service restoration. The TOC Critical Incident Management Process should define roles and responsibilities required for TOC Critical Incident Management. TOC Shift Supervisors shall lead and manage TOC Critical Incidents, to include shift turnovers as necessary.

4.5.3 ANALYSIS AND PROBLEM MANAGEMENT REPORTING

The contractor shall provide Enterprise Analysis Support. Support shall include but is not limited to ensuring accurate incident reports and analysis of these reports to determine root cause and emerging or chronic trends in the environment. Support shall also include technical requirements analysis and recommendations to address recurring issue impacting the USCIS Enterprise. The contractor shall record and document all technical analysis and recommendations that are developed to improve USCIS applications, services, and network infrastructure. The contractor shall routinely coordinate and provide updates to the USCIS Problem Management team as required.

4.6 COORDINATION

The contractor shall coordinate and collaborate with various entities outside of the TOC and/or USCIS. The contractor shall be responsible to work with the following external entities to accept, resolve, or escalate incidents as required. These relationships include but are not limited to:

- Working with DHS on Wide Area Network (WAN) issues and jointly coordinating with the Network Operations Support Center (NOSC) and Enterprise Operations Center (EOC) entities
- Working with other components of the DHS where USCIS services may reside or may be shared. Examples would include US Immigration and Customs Enforcement (ICE), and Customs and Border Patrol (CBP) but is applicable to all DHS components
- Working with the USCIS Security Operations Center (SOC) on issues which span the responsible areas of both the TOC and the SOC (examples might include a security scan which created a denial of service)
- Coordinating information back and forth with the USCIS Enterprise Service Desk regarding outages and other end user support
- Working with USCIS Service Desk IT Field Support (ITFS) Engineers (FSE). FSE's are considered the end users at each site where USCIS devices reside. Coordination with the FSEs shall include managing read access to the remote devices and granting permissions for local repairs (aka touch maintenance), in coordination with and as an extension to the TOC
- Coordinating with the USCIS Engineering to ensure that Engineering Projects are properly transitioned before allowing the systems to operate on the USCIS Infrastructure
- Coordinating with the CIRT
- Coordinating with the USCIS deployment team, USCIS TISO mailbox (Circuit Logistics) for both new circuit installations, and restoring circuit outages
- Also, Watch Officer directed / ad-hoc requirements

4.6.1 SUPPORTING DHS CONTINGENCY AND EMERGENCY OPERATIONS

The contractor shall assign at least two (2) individuals to work at USCIS Headquarters in Camp Springs, Maryland. These individuals, on a normal business day, will conduct Technical Operations Center Support Services the same as other contract employees and will be included in shift planning for the TOC. The capability to provide TOC Support Services remotely will be available. In times of emergency, disaster operations, continuity of operations, or similar events, these individuals will serve as the principal technical liaisons between the DHS Government Watch Officers and provide USCIS TOC Support Services if the primary site is unavailable. The Government reserves the right to adjust staffing levels at USCIS HQC based on operational requirements.

4.6.2 CLOUD MIGRATION COORDINATION

The contractor shall support USCIS' migration to cloud services, as it relates to the Technical Operations Center. Support will include but may not be limited to coordination with components and third-party vendors, transfer of knowledge, data, and troubleshooting of issues.

The contractor shall monitor, support end to end visibility, and troubleshoot issues for all cloud hosted applications. The contractor shall maintain and update documentation including but not limited to KMs, Diagrams, etc. The contractor shall establish a system to monitor and report application uptime and traffic performance.

4.7 TASK 6 – POLICY INPUT

The contractor shall be responsible for maintaining and enforcing multiple operational policies. The contractor shall provide expert advice on policy formation and make recommendations. The contractor shall assist in the drafting and writing of these policies when requested. Technical policies are maintained in ServiceNow.

The contractor shall be responsible to create Discrepancy Report for any policy which is not clear, accurate, or does not serve to mitigate the risk or serve the purpose intended. The Discrepancy Report shall identify where the policy is lacking clarity and provide recommendations to remediate the weakness.

The policies below all are currently in existence and will not need to be created but will need to be updated.

4.7.1 CHANGE CONTROL POLICY

Change Control policies ensure that all modifications to the TOC baseline are documented, approved, and that they properly identify and mitigate risk. As part of change control, the contractor shall provide input to the USCIS Virtual Change Advisory Board (VCAB) when requested. The VCAB provides change oversight and quality control for proposed changes. The VCAB reviews changes, analyzes each change for identified risks, mitigation of those risks, and reasonableness of the change. The VCAB is also responsible for review and resolution of all Discrepancy Reports (DRs).

4.7.2 STANDARD OPERATING PROCEDURES

Each USCIS service supported by the USCIS TOC shall have a Standard Operating Procedure (SOP) that describes procedures to monitor, manage, and support the USCIS applications, services, and network infrastructure. The intention of the SOP is to ensure that a consistent process is performed by each member of the USCIS TOC for each major category of issue. The SOP describes a process flow and often refers to other more detailed documents that describe in more detail how to complete a task within the flow. The whole of these documents comprise the TOC

Playbook maintained by the TOC and Knowledge Management Articles maintained in ServiceNow. The contractor shall be responsible to document these processes within both the TOC Playbook and ServiceNow.

4.7.3 TRANSITION AND ACCEPTANCE POLICY (FROM DEVELOPMENT TO OPERATIONS)

The contractor shall be responsible for the maintenance and enforcement of transition and acceptance policies. Transition policies provide rules and guidelines that must be present to transition a service, site, or device from development to operational. Transition policies include requirements for training, documentation, work that must be performed by a separate contractor or the network engineering team, and escalation policies as required by the government.

Acceptance policies provide rules and procedures to complete acceptance of a service, site, or device from another group to the operations group. Acceptance policies include the closure of all transition policy issues by ensuring acceptance criteria is complete. These documents are maintained separately but must be made available on request.

4.7.4 ESCALATION AND NOTIFICATION POLICY

The contractor shall be responsible for the maintenance and enforcement of escalation and notification policies. Escalation policies include levels of support, points of contact, periods to escalate to the next level and notification requirements. These policies create a support structure for the USCIS TOC by recruiting additional resources to solve complex incidents and engaging the CIRT/CSIRT when appropriate.

Notification policies include classification of incidents per the Impact and Urgency Matrix, points of contact, and notification procedures to follow when incidents occur. The intention of notification policies is to provide a consistent and rapid notification system to management. These policies and procedures are published and maintained in ServiceNow.

4.7.5 MAINTENANCE AND UPGRADE POLICY

The contractor shall be responsible for the enforcement of maintenance and upgrade policies. Maintenance policies include consistent operating system versions (as applicable), consistent configuration settings across similar devices (as applicable), and enforcement of ongoing audit and baseline tasks. Consistency and data integrity are important in maintaining a standardized environment and are valuable to the USCIS program. The most appropriate enterprise solution(s) shall be leveraged for this purpose (e.g. Cisco DNAC, SolarWinds). Upgrade policies include valid reasons to upgrade, upgrade processes, testing, and validation.

4.8 TASK 7 – REPORTING

The contractor shall be responsible for creating, maintaining, and communicating all USCIS TOC reports. The contractor shall further be responsible for the maintenance and enforcement of all Report Communication Plans. The Report Communication Plan describes how each type of report is delivered to its intended audience. Each report generated must have a report communication plan. The intention of this plan is to ensure that reported data reaches its intended audience.

Some reports require different methods of delivery. Delivery methods include ticket generation, phone calls, emails, spreadsheets, and Word documents. The Report Communication plan also details the frequency and conditions of the report. The contractor shall maintain the Report Communication Plan in ServiceNow. A list of the required reports, with a brief description, is listed as follows:

- **Audit Report** - defines all operational devices and services supported by the TOC (See Appendices A and C respectively for a full list of devices and services). Defining the scope of devices and services is critical to the success of the TOC because it must plan and manage its resources based on this data. Audit Reports include the following information:

    - Summary of changes in audited data from the previous audit report.
    - Additions and deletions of TOC supported devices, sites, or services from the previous audit report.
    - Number and size of physical sites in the USCIS network.
    - Number and type of assets in the USCIS network.
    - Number and type of supported services in the USCIS network.
    - Physical audit data per site
        - Who performed the last audit?
        - Date of the last audit
        - Audit results
    - Service availability report for the USCIS Enterprise.
        - Up/down time for devices monitored, with percentage up and cumulative percentage for the enterprise.
    - TOC incident handling QA report.
    - Reports associated with determining the effectiveness of any enterprise network solution.
    - Identify single points of failure and make recommendations to rectify.
    - Devices and system monitored, organized by system/application if applicable or by site if not applicable.
    - Comparison of devices monitored with Domain Name Servers, Configuration Management Database, and inventory lists.

- **Baseline Report** - describes the current state of every operational USCIS service defined in the audit report. The baseline report includes these major sections:

    - Current state of the service (Fault, Performance, Capacity, as described in sections 4.3.1 through 4.3.3).
    - Faults that occurred in the service since the previous baseline report.
    - Performance issues that occurred with the service since the previous baseline report.
    - Capacity issues that occurred or thresholds triggered since the previous baseline report.
    - Recommendations based on data provided in the report via an Incident Analysis Report (IAR).

- **Shift Transition Report** - describes open issues that constitute a “hand off” between one shift and another. The intention of this report is to ensure proper handling and communication of open incidents and issues from one shift to another

- **Incident Analysis Report(s) -** describe the lifecycle of a complex incident. The intention of this report is to create an accurate history of data and actions taken during an incident so that the audience of the report understands the issues clearly, to include what actions were taken, the root causes, what resolutions were attempted or accomplished, and recommendations for further action (if applicable). The audience for this type of report is the management chain and shall include an executive summary. The report

should retain all technical data as support for its conclusions, but the analysis of the data and recommendations are the primary motivation for the report. This report may include an After-Action Review (AAR) for cases where incidents did not get resolved as intended. AARs may generate Discrepancy Reports (DRs) depending on the problems identified during incident management. USCIS management may request AARs. The goal of the AAR is to identify issues that occurred during incident management, analyze the issues, and recommend solutions to mitigate risks for future incidents

- **Notification Report(s) -** Notification reports are smaller incremental reports that track an incident. Notification reports communicate to personnel as defined in the notification policies. The intention of a notification report is to:
    - Describe the scope of the incident
    - Provide data that further identifies the symptoms and possible root cause (if available)
    - Identify the people or groups involved with resolving the incident, including conference numbers
    - Describe the actions taken to identify and/or resolve the incident
    - Record the result of actions taken
    - Document any plans to continue resolution of the incident

  Often the data that first describes an incident is not accurate during the investigation. Each updated notification report reflects the previous and current changes to the data. The ultimate result of the notification reports that track a resolved incident is to provide adequate data for use in the Incident Analysis Report

- **Technical Support, Report Clarification and Recommendations to Improve Reports and Processes -** The contractor shall be responsible for providing technical support and report clarification for all reports. Sometimes a report contains unclear information or is missing detail requested by management. The intention of this section is to ensure that the information provided in all reports is traceable back to its source (either automated or personal), and reproducible (as applicable – the intention is to provide data integrity in the report). The contractor shall be responsible for the ongoing improvement of reports and report processes. Sometimes there are many questions derived from the same report. The contractor shall be responsible for identifying these trends and recommending solutions, including clarity, format, and processes to better serve the audiences of the reports.

4.9 TASK 8 - PROGRAM MANAGEMENT

The Contractor shall provide Program Management support for planning, execution, and completion of all program activities in accordance with best program management practices. While USCIS will provide management oversight, it is the responsibility of the Contractor to manage all corporate resources and supervise all Contractor staff in the performance of all work on this Task Order. The Contractor shall assign a Program Manager (PM) to this task who will manage the day-to-day activities of the Contractor staff. The contractor will establish the Program Management Office (PMO) at Stennis Space Center, Mississippi and will be available to meet, coordinate, monitor and report program and project management activities on a 24/7/365 basis.

The Contractor Program Manager shall be an employee of the Prime Contractor and have responsibility for the accomplishment of the Task Order. The Program Manager shall organize, direct, and coordinate the planning and execution of all activities, review the work of subordinates, including subcontractors, and ensure that the schedule, performance parameters, and reporting responsibilities are met. The Program Manager shall integrate the Contractor's management and technical activities across this Task Order to ensure they are consistent.

The Contractor's Program Manager shall be the primary interface with the USCIS Program Manager or designee. The Program Manager shall establish program management operations within 30-days of the Notice-To-Proceed (NTP). Program Management Operations are defined as a PM being assigned a permanent place of duty with telephonic and computer communications being established and the PM is prepared to meet the following requirements:

- Be the single Point Of Contact (POC) responsible for all performance, services, objectives, tasks and deliverables under this PWS
- Manage resources and supervise contractor staff in the performance of all work on this PWS
- Be responsible for the successful execution of the PWS tasks
- Organize, direct, and coordinate planning and execution of all PWS activities
- Ensure that the schedule, standards, reporting, and subcontract management responsibilities are met
- Identify and correct deficiencies and actively pursue solutions to correct deficiencies
- Be the primary interface with the Contracting Officer (CO), Contracting Officer's Representative (COR) and Government Program Manager
- Meet weekly with the Government Program Manager and COR
- Attend status meetings (includes cross-functional teams)
- Attend, create, manage project teams and report (as requested) project team status
- Identify qualified key personnel and leads (to include project teams)
- Maintain, track and report performance requirements
- Prepare and present quarterly Program Management Reviews (PMR) which will cover at a minimum, the program's status on cost, schedule, performance, risk management and status of deliverables and projects
- Provide a monthly Program Manager's Report detailing work accomplished, major tasks planned, personnel assigned, EOD suitability and security clearance status and other pertinent work detail to assist the TOC Federal Manager in understanding the labor-hours, time and materials hours (surge capacity) delivered
- Provide customer satisfaction oversight, corrective action implementation and program management support to resolve actual or customer perceived discrepancies in service

All lead personnel on the Task Order shall possess not only management skills, but technical skills as well and be hands-on executors, rather than just managers.

Independently of the number, and size of subcontractors the prime Contractor partners with, the Contractor shall present a united team to the Government.

At the request of the COR, the Government Program Manager, or a Government Technical Lead, the Contractor shall be required to prepare briefing materials, deliver briefings, participate in meetings with USCIS organizations and/or external organizations, and present program content. The Contractor shall develop, as necessary, written recommendations, oral presentations and/or executive briefing materials.

The following meetings are mandatory for the Contractor to attend and will be scheduled by the Government:

- Task Order Kick-Off meeting

- Technical Kick-Off meeting
- Weekly status meeting with Government staff
    - The Contractor PM and technical leads shall participate in person at the location designated by the Government
- Other ad-hoc meetings scheduled by USCIS senior leadership or Government team

The Contractor will be required to interact with multiple other contractor teams. The Government expects full Contractor cooperation, proper meeting attendance, and good faith efforts to accomplish joint work.

4.10 TASK 9 – SURGE SUPPORT (OPTIONAL T&M)

USCIS requires the ability to respond to emerging technology and trends that may benefit the customer. Surge support should be staffed with subject matter experts and/or journeyman level engineers. Trends may include, but are not limited to, technologies such as process automation, artificial intelligence operations (AIOps), and machine learning. Surge capability may be required to provide insight into technological advances as they arise. Surge capability may include how technological advances may benefit enterprise operations and provide support in integrating technologies into the Agency's landscape, as it deems necessary. War rooms, tiger teams and specialized groups may be stood-up to address and resolve critical issues and to discover, create, upgrade, and migrate these technologies. Reports, diagrams, and white papers produced during these meetings are considered government property and may be incorporated into the Technical Operations Center Playbook, a knowledge management article (KM) and/or USCIS' Information Technology Service Management (ITSM) tool at the government's discretion.

5 PERFORMANCE REQUIREMENTS

The Government will use the below performance standards to evaluate the Contractor's performance.

Performance Requirements Summary

PRS #	Required Services	PWS Reference	Performance Standard	Performance Level
1	Data Collection – Monitoring coverage/visibility of network devices and enterprise systems and applications	4.2.2	Number of devices monitored	≥ 97% of devices monitored 97% of the time

PRS #	Required Services	PWS Reference	Performance Standard	Performance Level
2	Data Collection - Uptime for devices and services, individual and cumulative.	4.2.2	System, Server, Network, Storage, and Infrastructure devices are available and operational except during scheduled maintenance	≥ 99.5% of devices described in the Performance Standard section are up during period.
3	Incident Response - Receipt of call and opening of incident ticket	4.4	≤ 15 Minutes	≥ 90% of the number of incidents within the time standard
4	Incident Escalation – Calling the on-call staff and issuing the incident ticket	4.4.1	≤ 30 minutes	≥ 95% of the number of incidents within the time standard
5	Incident Service Response – Service problem (Large Site – Resolution)	4.4	≤ 1 Hour	≥ 20% of the number of incidents within the required time
6	Incident Service Response - Service Problem (Large Site – Resolution)	4.4	≤ 4 Hours	≥ 50% of the number of incidents within the required time

PRS #	Required Services	PWS Reference	Performance Standard	Performance Level
7	Incident Service Response - Service Problem (Large Site – Resolution	4.4	≤ 24 Hours	≥ 50% of the number of incidents within the required time
8	Incident Service Response – Service Problem (Small Site – Resolution)	4.4	≤ 4 Hours	≥ 65% of the number of incidents within the required time
9	Incident Service Response – Service Problem (Small Site – Resolution)	4.4	≤ 24 Hours	≥ 95% of the number of incidents within the required time
10	Notification Reports - Escalation of Incidents and Services to the TOC (Network / Systems / Applications)	4.6.4	≤ 15 Minutes	≥ 75% of the number of incidents within the time standard
11	Notification Reports - Escalation of Incidents and Services to the TOC (Network / Systems / Applications)	4.6.4	≤ 30 minutes	≥ 95% of the number of closed incidents within the time standard

PRS #	Required Services	PWS Reference	Performance Standard	Performance Level
12	Notification Reports - Escalation of Incidents and Services from the TOC to the CIRT/CSIRT (Networks / Systems / Applications)	4.6.4	≤15 Minutes	≥ 75% of the number of incidents within the time standard
13	Notification Reports - Escalation of Incidents and Services from the TOC to the CIRT/CSIRT (Network / Systems / Applications)	4.6.4	≤ 30 Minutes	≥ 95% of the number of incidents within the time standard
14	Notification Reports - Escalation of Incidents and Services from the TOC to CIRT / CSIRT (Information Assurance & Security	4.6.4	≤15 Minutes	≥ 75% of the number of incidents within the time standard

PRS #	Required Services	PWS Reference	Performance Standard	Performance Level
15	Notification Reports - Escalation of Incidents and Services from the TOC to CIRT / CSIRT (Information Assurance & Security)	4.6.4	≤ 20 Minutes	≥ 95% of the number of incidents within the time standard
16	Notification Reports - Escalation of Incidents and Services from the TOC to DHS, The EOC or a Vendor (Information Assurance & Security)	4.6.4	≤15 Minutes	≥ 75% of the number of incidents within the time standard
17	Notification Reports - Escalation of Incidents and Services from the TOC to DHS, the EOC or a Vendor (Information Assurance & Security)	4.6.4	≤ 20 Minutes	≥ 95% of the number of incidents within the time standard

.

6 TASK ORDER ADMINISTRATION

6.1 DELIVERABLES

The Contractor shall submit the deliverables that are indicated in the table below to the Government Program Manager (PM), Contracting Officer Representative (COR), and Contracting Officer Technical Representative (COTR).

The Contractor shall provide all necessary personnel and deliverables based on the required delivery date(s) established by mutual agreement between the Government and the Contractor in the Task Order.

Upon receipt of the Government comments, the Contractor shall, within 5 business days, rectify the situation and re-submit the Task Order deliverable(s) if it is not a "draft" deliverable. If it is a "draft" deliverable, the Contractor shall rectify the situation before the next scheduled submission of this deliverable.

6.2 SCHEDULE OF DELIVERABLES

The table below aggregates all the deliverables that are part of this Task Order:

Deliverables			
Reference	**Requirement**	**Frequency**	**Due Dates**
	Post-Award Conference	Once and upon Option renewal?	Upon issue of NTP
4.8	Program Management Review (PMR)	Quarterly	NLT the 10th of the following month
4.8	Program Manager's Report	Monthly	NLT the 10th of the following month
4.1	Preliminary Transition Plan	Once and upon Option renewal?	With proposal
4.1	Final Transition Plan	Once and upon Option renewal?	15-days after award
4.2.1	Unauthorized Change Report	Daily	NLT than 10 am for the activity of the previous day
4.2.3	Discrepancy Report for Implementation Services	As needed when a discrepancy occurs	NLT 2 business days after discrepancy
4.3.5.3	Report on Devices Monitored	Quarterly	NLT the 10th of the following month

Deliverables			
Reference	**Requirement**	**Frequency**	**Due Dates**
4.4.1	After Action Report	As needed when an escalation occurs.	As needed when an escalation occurs.
4.6	Discrepancy Report for Policy or Procedure	As required whenever the policy is not clear, accurate, or does not serve to mitigate the risk or serve the purpose intended	As required whenever the policy is not clear, accurate, or does not serve to mitigate the risk or serve the purpose intended
	Audit Report	Monthly	NLT the 10th of the following month
4.7	Baseline Report	Weekly	NLT 2 business days after change
4.7	Shift Transition Report	At the end of each shift	At the end of each shift
4.7	Incident Analysis Report	Within one business day of an applicable incident or request by the Government TOC Section Chief / Watch Officer	Within one business day of an applicable incident or request by the Government TOC Section Chief / Watch Officer
4.7	Notification Report	IAW the Incident Management Process	IAW the Incident Management Process
6.6	Government Property Report	Annually	NLT 15 business days after receipt of GFP
6.10	Telework Plan	Once, or as requested by Government TOC Section Chief	in the Final Transition Plan
4.7	COOP/Emergency Plan	Bi-Annually or upon request by the Government TOC Section Chief	Within the Final Transition Plan and bi-annual updates
4.3	Technical Operations Center (TOC) Dashboard	IAW the Incident Management Process	IAW the Incident Management Process

6.3 PLACE OF PERFORMANCE

Work is to be performed at the USCIS TOC which is to be located within the Enterprise Operations Center (EOC) at Stennis Space Center, Mississippi, and in the National Capital Region at or USCIS HQC Camp Springs, MD. Both are government owned facilities.

6.4 PERIOD OF PERFORMANCE

The Period of Performance for this Task Order will be:

Base Period: 10/01/2025 – 09/30/2026
Option 1: 10/01/2026 – 09/30/2027
Option 2: 10/01/2027 – 09/30/2028
Option 3: 10/01/2028 – 09/30/2029
Option 4: 10/01/2029 – 09/30/2030

6.5 KEY PERSONNEL

The following personnel are considered key personnel and shall possess the following skills, level of experience, and certifications. The required 5 years of experience for Lead Key Personnel shall be in the positions equal or comparable to the position the person will hold on this contract.

Labor Category	Role on the Program	Responsibilities	Required Certification(s)
Program Manager (PM) *Information Technology Project Manager* *Labor ID # 284*	Provide high-quality project and program management standards across the whole project lifecycle. Advise clients on the project cost, program, risks and issues. Lead and manage multi-disciplinary professional teams.	Plan, initiate, and manage information technology (IT) projects. Lead and guide the work of technical staff. Serve as liaison between business and technical aspects of projects. Plan project stages and assess business implications for each stage. Monitor progress to assure deadlines, standards, and cost targets are met.	Bachelor's Degree or 10+ years IT experience; Minimum of 5+ years of IT Project Management experience; Project Management Professional (PMP) or equivalent certification; Certification in at least one of the following: CCNP; CCIE; MCITP/MCSE CISSP or equivalent.

Labor Category	Role on the Program	Responsibilities	Required Certification(s)
TOC Operations Manager/Deputy PM *Information Technology Project Manager* *Labor ID # 284*	Provide high-quality project and program management standards across the whole project lifecycle. Advise clients on the project cost, program, risks and issues. Lead and manage multi-disciplinary professional teams.	Plan, initiate, and manage information technology (IT) projects. Lead and guide the work of technical staff. Serve as liaison between business and technical aspects of projects. Plan project stages and assess business implications for each stage. Monitor progress to assure deadlines, standards, and cost targets are met.	Bachelor's Degree or 10+ years IT experience; Minimum of 5+ years of IT Project Management experience; Project Management Professional (PMP) or equivalent certification; Certification in at least one of the following: CCNP; CCIE; MCITP/MCSE CISSP or equivalent.
TOC Shift Supervisors Computer Network Support Specialist Labor ID # 153		Analyze, test, troubleshoot, and evaluate existing network systems, such as local area network (LAN), wide area network (WAN), and Internet systems or a segment of a network system. Perform network maintenance to ensure networks operate correctly with minimal interruption.	Minimum of 5+ years of IT experience as a lead or Subject Matter Expert (SME). Certification in at least one of the following: CCIE; CCNP; CISSP, RCSP; IBM Certified Deployment Professional; or MCITP/MCSE
Technical Project Management for TOC Emerging IT Projects / Technologies *Information Technology Project Manager* *Labor ID # 283*	Provide high-quality project and program management standards across the whole project lifecycle. Advise clients on the project cost, program, risks and issues. Lead and manage multi-disciplinary professional teams.	Plan, initiate, and manage information technology (IT) projects. Lead and guide the work of technical staff. Serve as liaison between business and technical aspects of projects. Plan project stages and assess business implications for each stage. Monitor progress to assure deadlines, standards, and cost targets are met.	Bachelor's Degree or 10+ years IT experience; Minimum of 5+ years of IT Project Management experience; Project Management Professional (PMP) or equivalent certification; Certification in at least one of the following: CCNP; CCIE; MCITP/MCSE CISSP or equivalent.

Labor Category	Role on the Program	Responsibilities	Required Certification(s)
Senior or SME Software Developer for Automation, Orchestrations, and AIOps Software Developer, Applications Labor ID # 313 / 314	Provide Senior or SME level skills in software development for automation, orchestration, and AIOps	Develop, create, and modify general computer applications software or specialized utility programs. Analyze user needs and develop software solutions. Design software or customize software for client use with the aim of optimizing operational efficiency. May analyze and design databases within an application area, working individually or coordinating database development as part of a team. May supervise computer programmers.	Minimum of 5+ years of IT experience as a lead or Subject Matter Expert (SME) with a proven record of successful software development and deployment projects. Certification in at least one of the following skills: Software Development, Automation and Orchestration, AIOps, or equivalent.
P&A Lead *Management Analyst* *Labor ID # 293/294*	P&A lead shall apply industry and Government standards and best practices in carrying out task supporting P&A functions.	Conduct organizational studies and evaluations, design systems and procedures, conduct work simplification and measurement studies, and prepare operations and procedures manuals to assist management in operating more efficiently and effectively. Includes program analysts and management consultants.	Minimum of 5+ years of IT experience as a lead or Subject Matter Expert (SME). Certification in at least one of the following: CCIE; CCNP; CISSP, RCSP; IBM Certified Deployment Professional; or MCITP/MCSE

The Contractor shall ensure the TOC is staffed with an adequate number of assigned personnel possessing the required certifications, qualifications, skills, background checks and experience.

The Contractor shall identify key personnel, provide a statement of qualifications and resume for each of these individuals upon task award and at any time a substitution is proposed. The statement of qualification will include a YES or NO declaration for meeting each of the requirements and the resume will show how the individual meets the requirements for the position.

6.6 GOVERNMENT FURNISHED PROPERTY

The Government will furnish the following property to the Contractor staff upon successful Enter-on-Duty (EOD):

Equipment/ Government Property	Date/Event Indicate when the GFP will be furnished	Date/Event Indicate when the GFP will be returned	Unit	Unit Acquisition Cost	Quantity	"As-is"
Laptop computer with power cord and desk lock	After EOD	Upon departure	EA	$1,800	TBD	TBD

Equipment/ Government Property	Date/Event Indicate when the GFP will be furnished	Date/Event Indicate when the GFP will be returned	Unit	Unit Acquisition Cost	Quantity	"As-is"
PIV card	After EOD	Upon departure	EA	$500	TBD	TBD
iPhone with screen protector, charging cord and protective case	After EOD	Upon Departure	EA	$1500	TBD	TBD

The Government will not be obligated to provide additional accessories for the laptop computers, such as monitors, computer bags, external mice, etc. The Contractor will be responsible for receipt, stewardship, and custody of the listed GFP until formally relieved of responsibility in accordance with FAR 52.245-1 *Government Property* and FAR 52.245-9 *Use and Charges.* The property may not be used for any non-task order purpose. The Contractor bears full responsibility for all loss of this property, whether accidental or purposeful, at full replacement value.

6.7 GOVERNMENT FURNISHED INFORMATION

At a minimum, the Government will provide the Contractor access to the following informational resources and support systems:

Informational Resource/ Systems	Date/Event Indicate when the SW will be furnished	Date/Event Indicate when the SW will be returned
System access – contractor staff will be provided access to USCIS systems. Access will be provided to staff based on job duties	Upon authorized EOD and full Background Investigation (BI) adjudication (required for access to Prod environment)	Access will be terminated upon contractor departure
DHS, USCIS Intranet and E-mail system	Upon EOD	Access will be terminated upon contractor departure

The Contractor will be exposed to additional informational resources while working with USCIS, such as DHS and USCIS policies and management directives, informational meetings, demonstrations by other programs and vendors, business SOPs, etc.

6.8 HOURS OF OPERATION

The Hours of Operation are 24 hours a day, 365 days a year. The Technical Operations Center is a mission essential organization and remains open through holidays and emergencies.

6.9 TRAVEL

Travel may be required in support of Program Management Reviews, Project Support and specific requirements based on Government need.

6.10 TELEWORK

The Contracting Officer Representative (COR) may authorize employees to telework in support of this Task Order for Emergency, or Disaster Recovery purposes (i.e. natural disasters, security issues/incidents) after the review and acceptance of the Contractor's Telework Plan by the Government TOC Section Chief and the COR. The Contractor's Contingency Operations Plan (COOP) is due with the Final Transition Plan. Prior to commencement of any teleworking activities, the Contractor shall provide the COR, Government TOC Section Chief, and the Government Contract Program Manager with an approved copy of the Telework Plan. The Government will not pay travel reimbursement for travel between a contractor authorized work site and Stennis Space Center, Mississippi.

6.11 ACCESSIBILITY REQUIREMENTS – SECTION 508

Section 508 Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when federal agencies develop, procure, maintain, or use Information and Communications Technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of federal employees and members of the public without disabilities.

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

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

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

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

Instructions to Offerors

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

Acceptance Criteria

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

6.12 PERSONNEL SECURITY REQUIREMENTS

TOC Personnel Security

- DHS/USCIS does not permit the use of non-U.S. Citizens in the performance of this contract or to access DHS/USCIS systems or information.
- All contractor personnel (including subcontractor personnel) must have favorably adjudicated background investigations commensurate with the sensitivity level of the position held before being granted access to DHS/USCIS sensitive information.
- In accordance with Section 4.2 of this work statement, at least 2 individuals per TOC shift will be available to assist in remediating issues involving the CSIRT. In the conduct of that work, personnel will be exposed to information up to the Secret level and must possess the appropriate clearance level.
- In accordance with paragraph 4.5.1 at least two and not more than 3 individuals under this contract will be assigned to work with DHS on Contingency and Emergency Operations. In the event of an emergency, personnel may be exposed to briefings, instructions and other information at the Secret level and must possess the appropriate clearance.
- Support and coordinate with appropriate organizations within DHS, including but not limited to the DHS SOC, the CIO, the CISO, the TOCs and SOCs, the DHS Inspector General (IG), Components, and law enforcement as appropriate.
    - At no time will uncleared personnel attempt to access the information or affected systems, unless explicitly authorized by the DHS CSO, the HSDN SOC, or the I&A SOC.
        - Ensure that only personnel cleared at the level of the spillage or higher handle the incident.
        - Report the incident to the DHS CSO, the HSDN SOC, or the I&A SOC without delay.
        - Initiate actions to isolate and contain the information to minimize damage and preserve evidence that may be required for damage assessment, risk assessment, law enforcement, or counterintelligence purposes.
- The contractor shall ensure its personnel have a validated need to access DHS/USCIS sensitive information and are granted the most restrictive set of access privileges needed for performance of authorized tasks.

- The contractor shall ensure that its personnel comply with applicable Rules of Behavior for all DHS/USCIS IT systems to which its personnel have been granted access privileges.
- The contractor shall implement procedures to ensure that system access privileges are revoked for contractor personnel whose employment is terminated or who are reassigned to other duties and no longer require access to DHS/USCIS sensitive information.
- The contractor shall conduct exit/de-brief interviews to ensure that contractor personnel who no longer require access to DHS/USCIS sensitive information understand their obligation not to discuss or disclose DHS/USCIS sensitive information to which they were granted access under this contract.

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 12958, Classified National Security Information, and supplementing directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service.

Any firm or business under contract with the Department of Homeland Security (DHS), which requires access to classified information, will require a facility security clearance commensurate with the level of access required. Firms that do not possess a facility clearance, or the requisite level of facility clearance, will be sponsored for a Department of Defense facility clearance.

SUITABILITY DETERMINATION

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

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information and/or classified information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the Position Designation Determination (PDD) for Contractor Personnel. The results of the position sensitivity analysis

shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-86, "Questionnaire for National Security Positions" via e-QIP:

- DHS Form 11000-6, "Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement"
- FD Form 258, "Fingerprint Card" **(2 copies)**
- Form DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
- Position Designation Determination for Contract Personnel Form
- Foreign National Relatives or Associates Statement
- OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
- ER-856, "Contract Employee Code Sheet"

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information and/or classified information has resided in the U.S. for three of the past five years, OSI PSD may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

Only U.S. citizens are eligible for employment on contracts requiring access to DHS Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued by the Social Security Administration.

VISIT AUTHORIZATION LETTER (VAL)

The Contractor is required to submit a VAL for those individuals who require access to classified information during performance on this contract and who have an active Personnel Security Clearance (PCL). The letter will be valid for a period not to exceed one year. If the requirement to access classified information no longer exists, or if access eligibility changes, OSI will be notified immediately. The VAL must be submitted to OSI PSD in accordance with, and contain information as required by, Chapter 6 of the NISPOM.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer's Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract. In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a contractor's reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than December 31st each year, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **USCIS Office Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-86 security questionnaire.

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Facility Security Officer. The individual will interface with OSI through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

Contractor employees who become eligible for access to classified National Security Information shall participate in annual USCIS NSI refresher briefings. Briefings be coordinated through the COR, PSD and the OSI Administrative Security Division.

In the event classified information is inadvertently received by a contractor who does not hold an active security clearance at the Secret level, a Government employee or Contractor with the appropriate security clearance equal

to or higher than the classified information received, will take possession of the material and shall safeguard and store the information in accordance with standards set forth in the NISPOM. The inadvertent disclosure will be immediately reported to their supervisor and then to the designated OSI Local Security Officer or OSI Field Security Manager for action as appropriate.

In the event classified information is inadvertently received by a contractor who does not hold an active security clearance at the Secret level, a Government employee or Contractor with the appropriate security clearance equal to or higher than the classified information received, will take possession of the material and shall safeguard and store the information in accordance with standards set forth in the NISPOM. The inadvertent disclosure will be immediately reported to the local USCIS TOC personnel for action.

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, SSN, email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII

Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

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

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

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

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

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include Social Security Number (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)

(2) Date of Birth (Month, Day, and Year)

(3) Citizenship or Immigration Status

(4) Ethnic or Religious Affiliation

(5) Sexual Orientation

(6) Criminal History

(7) Medical Information

(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

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

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

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

(1) 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 (SBU) 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 Protected Critical Infrastructure Information (PCII), Sensitive Security Information (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* (SPII) provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

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

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

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

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

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

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

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

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

providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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

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

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

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are

determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

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

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

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.
(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.
(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

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

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

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

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

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

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

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

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

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

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

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

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

(b) *Security Training Requirements*.

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

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

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

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

6.13 ENTERPRISE ARCHITECTURE (EA) COMPLIANCE LANGUAGE

DHS Enterprise Architecture (EA) Compliance

All solutions and services shall meet DHS Enterprise Architecture (EA) policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security (HLS) EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA principles
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile; all products are subject to DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the HLS EA TRM Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

7 APPENDIX – TOOLS AND SERVICES

The monitoring and configuration tools listed below are those which are either currently used or have been recently used by USCIS TOC. All tools are subject to change:

Monitoring/Configuration TOOLS:

- Cisco ISE - Cisco authentication, authorization, accounting server (Identity Services Engine)
- InfoBlox – DHCP, DNS and NTP
- Load Balancers – Provides redundancy and failover capabilities.
- Routers - Network device that allows for communication between LAN (Local Area Networks) Segments
- Switches - Network device that allows for communication within a LAN segment
- Ansible
- Cisco DNA Center - digital network architecture
- PowerBI – USCIS' system of record for performance and capacity management monitoring.
- Meraki – out of band network management
- SPLUNK
- Solarwinds Orion
- VMWare VELOCloud SD-WAN
- Grafana
- Amazon Web Services
- Microsoft Azure
- Power Automate (Microsoft)
- Aternity – End User workstation performance /apdex monitoring.
- Algosec - full policy lifecycle automation management solution
- ServiceNow – Ticketing, Knowledge Management articles, CR process and others
- Veeam Backup Enterprise Manager –
- New Relic

The services listed below are examples of services used by USCIS. All services are subject to change.

Application Support Services:

- Database Services (example Oracle, Microsoft SQL Server) excluding MS Access
- Web Services (Web servers and middleware applications)
- Server Hosting (AWS/AZURE)

Email

- Microsoft Office 365

End User Application Services: (Subject To Change)

•129CWR	CASE SCANNING PORTAL
•ADM	AR-11 Data Input System
•AHS	AAMVA Hub Services
•AIS	Architecture and Information Security
•AOS	Adoption Orchestration Services
•APMA	Accounts Public My Account
•Asset Manager	Asset Manager
•ATLAS+	ATLAS+
•Backstage	Backstage
•BADS	BIA [Board of Immigration Appeals] Appellate Decisions Search (BADS)

•BCPS	Badge and Credential Processing System
•BEQS	EGIS Business Enterprise Query System
•BHub	Benefits Hub
•BMT	Business Management Solutions/Budget Management Tool
•CAMINO	Case and Activity Management for International Operations
•CDMT	Card Management
•CIDR	Citizenship and Immigration Data Repository
•CIS2	Central Index System 2
•CLAIMS 3 LAN	Computer-Linked Application Information System 3.0 Local Area Network
•CMIS	Customer Management Information System
•CMS	Content Management Services
•COPS	Centralized Organization Provider Service
•CPMS	Customer Profile Management System/Biometric Enrollment Tool
•CPMS-SS	Customer Profile Management System - Support Service
•CRIS	Customer Relationship Interface System
•CSWP	Customer Service Web Portal
•CT	Common Tools
•DBIS	Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)
•D-NAT	Denaturalization
•Dolores	OPS Dashboard
•DSMS	Document & Supplies Management System
•ECC-CEC IVA	Enterprise Call Center - Customer Engagement Center - Intelligent Virtual Assistant
•ECC-CEC-IVRS	USCIS Enterprise Call Center Interactive Voice Response System
•ECHO	Enterprise Correspondence Handling Online
•EDMS	Enterprise Document Management System
•EFRS	Exam Fee Receipting System
•EGIS-RefDaaS	Reference Data as a Service (RefDaaS)
•ELIS	Electronic Immigration System
•Employee Profile	Employee Profile
•Encryption	EGIS Encryption
•EPMS	Enterprise Print Management Service
•EPS	Export Process Server
•ePULSE	Electronic Personnel Universally Linked System
•ERIA	El Rescate Index of Accountability
•ESB-CPMS-SS	Enterprise Service Bus – Customer Profile Management System Support Services
•ESS	EGIS Enterprise Document Management System Support Service
•eSTAT	Electronic Statistical Automated Activity Tracking
•E-Verify	E-Verify
•eWRTS	Electronic Working Reporting and Tracking System (eWRTS)
•FACCON	Facilities Connect
•FAMS	Facilities Automated Management System
•FIRST	FOIA Immigration Record System
•FOD Link	Field Operations Directorate (FOD) Link (FODLink)
•GitHub	GitHub
•Global	GLOBAL
•ICAM-Enterprise	Identity, Credential and Access Management
•ICMS	Interim Case Management Solution
•ICPS-CPSTR	Card Personalization System Technology Refreshment
•ICPS-SMI	Secure Mail Initiative
•ICTS	International Caseload Tracking System
•IDCMS	Investigations Division Case Management System
•INFACT	Investor File Adjudication Case Tracker
•ITAM	Information Technology Asset Management
•IVCS	Immigrant Visa Content Service
•JSON Forms	EGIS JSon Forms service
•LIS	EGIS Lockbox Intake Service
•MIDAS	Microfilm Digitization Application System
•MSI Map	Minority Serving Institution Map
•myE-Verify	myE-Verify
•myUSCIS	myUSCIS
•NASS	National Appointment Scheduling System
•NLETS	National Law Enforcement Telecommunications System
•NPWR	National Processing Workflow Repository
•O&M	EGIS ESB Operations and Maintenance
•OIT-HR Dashboard	Office of Information Technology Human Resources Dashboard
•OPTS	OSI Processes Tracking System

•OTF	Overtime Tracking Form
•Pangaea COI Tool	Pangaea Country of Origin Information Tool (Pangaea COI Tool)
•Passport Tracker	Passport Tracker
•Payments	EGIS Payments
•PC	Public Charge
•PCQS	Person Centric Query Service
•PCS	Person Centric Services
•QADB	Quality Assurance Data Base
•QUEUE	Quality Unit End User Evaluation
•RAD Case Manager	RAD Case Manager (RCM)
•RAILS	RAILS
•RASS	Refugee Asylum Support Service
•Rejects Tracker	Rejects Tracker
•ROSS2	Resource Optimization and Scheduling System
•SAVE	Electronic Immigration Status Verification
•Scheduler RoR	Scheduler RoR
•ServiceHub	serviceHUB
•SI	Service Center Operations Directorate (SCOPS) Intake
•SNow	ServiceNow
•SODA	Scan on Demand Application
•STARS	System for Tracking Activities, Relationships, & Services
•SVS	Status Verification System
•TA	Text Analytics
•UIP	Unified Immigration Portal
•VCS	Verification Information System Core Services
•VIBE+	Validation Instrument of Business Enterprises Plus
•VS	Verification Service
•VSS	Visa Support Services
•WDS	Work Distribution System

Enterprise Management Services:

- Configuration Control Services (example Cisco DNAC , Solarwinds)
- Network Authentication Services (example CISCO ISE)
- Network Performance Monitoring Services (example New Relic)
- Packet Tracing Services (example Wireshark)

InfoBlox – DHCP and DNS service