

**Statement of Work  
for  
Enterprise Network Services Technology  
Information Technology Field Service Support  
Network and Security Operations Center  
Technology Service Desk  
Program and Project Management Support**

**US Customs and Border Protection  
Office of Information Technology**

**HSBP1010F00278  
Attachment 1**

**TABLE OF CONTENTS**

1	PROJECT TITLE .....	3
2	BACKGROUND .....	3
2.1	Information Technology Field Services Support.....	3
2.2	Network and Security Operations Center, DHS OneNet.....	3
2.3	Technology Service Desk .....	3
2.4	Program and Project Management.....	3
3	SCOPE .....	3
3.1	Information Technology Field Services Support.....	3
3.2	Network and Security Operations Center, DHS OneNet.....	3
3.3	Technology Service Desk .....	3
3.4	Program and Project Management.....	3
3.4.1	Program and or Project Planning Services.....	3
3.4.1.1	Integrated Schedule Requirements .....	3
3.4.2	IT Investment Management .....	3
4	APPLICABLE DOCUMENTS.....	3
5	PERFORMANCE REQUIREMENTS .....	3
5.1	Information Technology Field Services Support.....	3
5.1.1	TECHNICAL PERFORMANCE REQUIREMENTS .....	3
5.1.1.1	TASK 1: System Management Support.....	3
5.1.1.2	TASK 2: Customer Service Support.....	3
5.1.1.3	TASK 3: Resource Management Support.....	3
5.1.1.4	TASK 4: Wide Area Network (WAN)/Local Area Network (LAN) Support.....	3
5.1.1.5	TASK 5: First Responders Support.....	3
5.1.1.6	TASK 6: Telecommunication Support .....	3
5.1.1.7	TASK 7: Facilities/Modernization Information Technology Infrastructure Support.....	3
5.1.1.8	TASK 8: Project Management Support and Deployment.....	3
5.1.1.9	TASK 9: International Support.....	3
5.1.1.10	TASK 10: Optional Level of Effort (LOE).....	3
5.1.1.11	TASK 11: Program Management and Administrative Services.....	3
5.1.2	TASK ORDER AND CONTRACT MANAGEMENT REQUIREMENTS.....	3
5.2	Network and Security Operations Center, DHS OneNet.....	3
5.2.1	GENERAL REQUIREMENTS.....	3
5.2.2	Project Management .....	3
5.2.2.1	Constraints .....	3
5.2.2.2	Transition Plan, if applicable .....	3
5.2.2.3	Network and Security Operations Center Support.....	3
5.2.2.4	NETWORK AND SECURITY OPERATIONS CENTER SUPPORT SERVICES .....	3
5.2.2.5	Network Management System Support .....	3
5.2.3	Systems Administration.....	3
5.3	Technology Service Desk .....	3
5.3.1	Support Services .....	3
5.3.2	General Services .....	3

5.3.3	Project Support.....	3
5.3.4	Password Services.....	3
5.4	Program and Project Management.....	3
5.4.1	Constraints .....	3
5.4.1.1	Operational Constraints .....	3
<b>6</b>	<b>TECHNICAL PERFORMANCE STANDARDS.....</b>	<b>3</b>
6.1	Information Technology Field Services Support.....	3
6.2	Network and Security Operations Center, DHS OneNet.....	3
6.2.1	Performance Metrics.....	3
6.2.2	Standard Operating Procedures (SOPs), Tactics Techniques Procedures (TTPs) and Operating Instructions (OIs) .....	3
6.2.2.1	Service Level Objectives .....	3
6.3	Technology Service Desk.....	3
6.3.1	Performance Measures.....	3
6.4	Program and Project Management.....	3
<b>7</b>	<b>Contract type .....</b>	<b>3</b>
<b>8</b>	<b>DELIVERABLES AND DELIVERY SCHEDULE .....</b>	<b>3</b>
8.1	Information Technology Field Services Support.....	3
8.2	Network and Security Operations Center, DHS OneNet.....	3
8.2.1	Reporting Requirements .....	3
8.2.1.1	Daily Situational Awareness Brief.....	3
8.2.1.2	Daily Status Report.....	3
8.2.1.3	Weekly Status Reports (Bandwidth, Ticketing, Budget, Personnel).....	3
8.2.1.4	Monthly Program review Reports (Bandwidth, Ticketing, Budget, Personnel).....	3
8.2.2	Briefing/Meetings .....	3
8.2.3	Periodic Meetings .....	3
8.2.4	Deliverables Table .....	3
8.2.4.1	Deliverable Requirements Delivery Schedule .....	3
8.2.4.2	Reporting Requirements Delivery Schedule.....	3
8.3	Program and Project Management.....	3
8.3.1	Project SELC Artifacts .....	3
8.3.2	Project Cost Management Artifacts.....	3
8.3.3	Project Schedule Management Artifacts.....	3
8.3.4	Integrated Master ITP Program Schedule.....	3
8.3.5	Briefings, White Papers, Presentations.....	3
8.3.6	Program/Project Meetings .....	3
8.3.7	Standard Operating Procedures (SOPs), Tactics Techniques Procedures (TTPs) and Operating Instructions (OIs) .....	3
8.3.8	Reporting Requirements .....	3
8.3.8.1	OneNet Circuit Order Status Report.....	3
8.3.8.2	Weekly Project Status Reports.....	3
8.3.8.3	Project Program Management Reviews.....	3
8.3.8.4	Periodic Contract Meetings.....	3
8.3.8.5	Task Order Status Reports .....	3
8.3.9	Program Management and Administrative Services.....	3
8.3.10	Quality Control .....	3
8.3.11	Project SELC Artifacts .....	3

8.3.12	Project Cost Management Artifacts.....	3
8.3.13	Project Schedule Management Artifacts.....	3
8.3.14	Integrated Master ITP Program Schedule.....	3
8.3.15	Briefings, White Papers, Presentations.....	3
8.3.16	Program/Project Meetings.....	3
8.3.17	Standard Operating Procedures (SOPs), Tactics Techniques Procedures (TTPs) and Operating Instructions (OIs).....	3
8.3.18	OneNet Circuit Order Status Report.....	3
8.3.19	Weekly Project Status Reports.....	3
8.3.20	Project Program Management Reviews.....	3
8.3.21	Periodic Contract Meetings.....	3
8.3.22	Task Order Status Reports.....	3
8.3.23	Deliverables Tables.....	3
8.3.24	Deliverable Requirements Delivery Schedule – Technical Point of Contact(s) (TPOC) will be designated at the kick-off of each project.....	3
8.3.25	8.11.2 Reporting Requirements Delivery Schedule.....	3
8.4	Acceptance Requirements of Deliverables.....	3
9	<b>INVOICE REQUIREMENTS/PERIOD OF INVOICE.....</b>	<b>3</b>
9.1	Travel.....	3
9.2	Other Direct Costs.....	3
9.3	Project Accounting Reports.....	3
9.4	Earned Value Management and Reporting.....	3
10	<b>GOVERNMENT-FURNISHED PROPERTY, EQUIPMENT AND INFORMATION.....</b>	<b>3</b>
10.1	PROPERTY.....	3
10.2	EQUIPMENT.....	3
10.2.1	Information Technology Field Services Support.....	3
10.2.1.1	Government Furnished Tools.....	3
10.2.2	Network and Security Operations Center, DHS OneNet.....	3
10.2.2.1	Government Furnished Tools.....	3
10.2.3	Technology Service Desk.....	3
10.2.4	Program and Project Management.....	3
10.3	INFORMATION.....	3
10.3.1	Information Technology Field Services Support.....	3
10.3.2	Network and Security Operations Center, DHS OneNet.....	3
10.3.2.1	Storage and Management of Government Finished Information.....	3
10.3.3	Technology Service Desk.....	3
10.3.4	Program and Project Management.....	3
10.4	Property.....	3
10.4.1	Government Owned Vehicles.....	3
11	<b>PLACE OF PERFORMANCE.....</b>	<b>3</b>
12	<b>PERIOD OF PERFORMANCE.....</b>	<b>3</b>
13	<b>STANDARD CLAUSES.....</b>	<b>3</b>
14	<b>CONTRACTOR EMPLOYEES.....</b>	<b>3</b>
14.1	KEY PERSONNEL.....	3
14.2	PERSONNEL RELEVANT KNOWLEDGE, ABILITIES, AND SKILLS.....	3
14.2.1	Information Technology Field Services Support.....	3

14.2.2	Network and Security Operations Center, DHS OneNet.....	3
14.3	Technology Service Desk .....	3
14.4	Program and Project Management.....	3
14.4.1	The Program Manager .....	3
14.5	WORK HOURS.....	3
14.6	OVERTIME.....	3
14.7	IDENTIFICATION BADGES.....	3
14.8	CONTRACTOR IDENTIFICATION .....	3
14.9	MANDATORY AND OTHER TRAINING .....	3
14.10	EMPLOYEE CONDUCT.....	3
14.10.1	Contractor Input and Tracking.....	3
15	GOVERNMENT POINTS OF CONTACT (POC) .....	3
	ATTACHMENT 1 - ACRONYM LIST:.....	3
	ATTACHMENT 2 - FIELD SUPPORT APPROVED SOP LIST.....	3
	Addendum A policies .....	3
	Addendum B standard terms and conditions.....	3
	personnel security .....	3
	Addendum C COTR and task monitor list.....	3

## **1 PROJECT TITLE**

CBP Enterprise Network Services Technology: Information Technology Field Services Support, Network and Security Operations Center, Technology Service Desk, and Program and Project Management Support

## **2 BACKGROUND**

CBP is responsible for the protection of the United States' borders, its citizens and its commerce. Over the past 20 years, CBP has been the nation's frontline defense in countering narcotics smuggling. CBP is now performing an increasingly demanding role in countering terrorist activities characterized by attempted smuggling of materials for weapons of mass destruction and infiltration of terrorists at Ports of Entry. To enforce the laws, CBP relies on vigilance coupled with technology.

CBP's Office of Information and Technology (OIT) is charged with providing global support for all information technology to ensure CBP users, as well as other authorized enforcement agencies and authorized members of the Trade, have access to those systems necessary for supporting their mission. Additionally, OIT is responsible for architecture, design, engineering and management of the CBP network infrastructure as well as the DHS OneNet wide area network (WAN).

### **2.1 Information Technology Field Services Support**

CBP utilizes intrusion detection systems, video surveillance, land vehicles, boats, aircraft, and foot patrol in a coordinated fashion to protect our borders and secure our nation against terrorism and drug trafficking. CBP also utilizes technologically advanced targeting systems to better identify people who may pose a risk, as well as automated systems to identify cargo that may pose a threat while expediting legitimate trade.

Field Support's mission is to support the critical systems which secure the United States with a superior integrated team of Field Deployment Engineers and Field Technology Officers. A large amount of technological hardware and applications are used in the collection and dissemination of information that allows CBP to be successful. Field Support provides:

- Technical solutions, support and expertise by installing Local Area Networks (LAN) and Wide Area Networks (WAN),
- Installations, testing and upgrades for equipment and software,
- Site surveys to assess needs,
- Day-to-day Tier 1 and 2 IT support (LAN, PC, telecommunications, etc.) ensuring operability.

### **2.2 Network and Security Operations Center, DHS OneNet**

The Network and Security Operations Center (NSO) is a 24x7x365 place of operations that provides network- and security- engineering operations support, problem identification, troubleshooting, and maintenance for CBP LAN, MAN, and WAN (OneNet). The NSO is the focal point for network troubleshooting, and updating, firewall, router and domain name management, performance monitoring, and coordination with affiliated networks. The NSO is responsible for providing network fault and performance monitoring, network utilization,

network availability, trend analysis, performance modeling, capacity planning, problem tracking and escalation, problem reports and documentations, and Quality of Service (QOS). The NSO is positioned at two locations, Springfield, Virginia and Orlando, Florida, and is structured as an active/active operation. The active/active operation provides for increased situational awareness, increased CBP/DHS OneNet availability, and the ability to ensure continuity of operations should something happen to the other location. The network environment, major types of equipment, consist of Cisco core and edge Routers, Switches, and Firewalls. Proxy Firewall appliances are used for edge devices to the Internet. The NSO is responsible for providing support to approximately 1,800 offices throughout the world that access DHS/CBP LAN, MAN and/or WAN "OneNet".

### **2.3 Technology Service Desk**

The Technology Service Desk (TSD) is the initial single point of contact for CBP and its customers. The contractor shall provide telephonic support for CBP and its customers twenty-four hours a day, seven days a week, 365 days a year. The contractor shall open and resolve incident or service request record in Remedy for all incoming request, i.e, calls, faxes, emails, voice mails, and automated monitored system alerts. The contractor shall perform technical support in accordance with requirements within this SOW.

### **2.4 Program and Project Management**

The Information Technology Program's (ITP), within OIT's Enterprise Networks and Technology Support Division (ENTS) manages projects associated with the modernization of specialized and general-purpose technology infrastructure that support CBPs mission across approximately 2,000 sites and 65,000+ employees and contractors, such as eMail System conversion, implementation of Windows LAN/WAN Directory Services, implementation of network and IT infrastructure redundancy, upgrade of PC desktop hardware and desktop Operating System software, LAN server infrastructure upgrades and migration to alternative LAN Operating System software, development and deployment of passport reader, fingerprint scanner and evolving technologies that support border security. The scale of projects managed by the ITP include small, single site projects to large, global enterprise projects with independent project lifecycle durations of several months to multiple-years. Throughout the lifecycle of its projects, the ITP performs program analysis and project management activities to assure completion of project planning, execution, control and completion of activities and deliverables to successfully achieve project completion.

During the course of managing its projects lifecycles, the ITP interfaces with stakeholders throughout DHS, business trade community, other federal departments/agencies, and commercial vendors/entities on a daily basis in the performance of IT project management responsibilities.

Through the ITP, OIT seeks to:

- Identify commonality and interdependencies of cross-organization IT infrastructure requirements for consolidation and aggregation into planned or on-going projects, and to plan and develop integrated deployment schedules where common project attributes are merged

- Curtail time-intensive repetitive workloads by introducing technology strategies that simplify and accelerate processes
- Reduce total CBP IT costs through program consolidation and standardization of project tasks
- Maintain a low total cost of ownership of IT assets

Though the ITP staff does not directly perform all project development activities, i.e. systems/application engineering, security certification, application/system testing, deployment, it is responsible for the overall project management, project control, and project performance/status reporting of each of its projects.

As part of the initiation of new projects, along with the development of project cost estimates, ITP staffs assess project team skill sets and identify project management support staff needs. These assessments determine the best utilization of existing and supplemental staff needs required to perform and accomplish project objectives. As projects emerge, supplemental staffing needs, along with project funding, become the basis for establishing increased optional level of effort support included within this task order.

### **3 SCOPE**

#### **3.1 Information Technology Field Services Support**

The requirement of this Statement of Work is to obtain contractor technical support services for CBP in the following principle technical areas:

- Task 1: Systems Management Support
- Task 2: Customer Service Support
- Task 3: Resource Management Support
- Task 4: WAN/LAN Support
- Task 5: First Responder Support
- Task 6: Telecommunications Support
- Task 7: Facilities/Modernization Information Technology Infrastructure Support
- Task 8: Project Management Support and Deployment
- Task 9: International Support
- Task 10: Optional Level of Effort Support
- Task 11: Program Management and Administrative Services

The Contractor is also expected to provide task order or contract management support.

Contractor employees under this Statement of Work shall provide high-quality technical solutions, support, and expertise to all Customs and Border Protection (CBP) sites both nationally and internationally by means of installing Local Area Networks (LAN) and Wide Area Networks (WAN), performing testing, installations, upgrades for equipment and software, and site surveys to assess needs and to be responsive to increasing technical requirements. The

contractor shall provide a service strategy, service design, service transition, service operation and continual service improvement following the Information Technology Infrastructure Library (ITIL) methodology. The contractor will be assigned to projects of varying size and scope by the government with the expectation of performing all required tasks, not limited to design, procurement, and implementation.

Our goal is to enhance security at our nation's borders, via the deployment of the latest IT Technology support to approximately 56,000 users at roughly 1,700 CBP nationwide LAN sites. This effort is intended to ensure the continuing operability of CBP's Information Technology infrastructure. CBP has historically used a mix of government and contractor personnel to provide these services nationwide. All services and deliverables performed by contractor will be in accordance with current CBP standards and applicable documents.

### **3.2 Network and Security Operations Center, DHS OneNet**

The Contractor shall provide network telecommunications, network engineering Network Management, Network Firewall Engineering services and project support services to the Network and Security Operations Branch, to include but not limited to, the CBP LAN, MAN and DHS WAN environment and its data centers. The NSO is a 24x7x365 center that operates in the confines of a secure facility, organized, staffed, and equipped to manage Network Operations and Maintenance functions that have relevance across an enterprise. The contractor shall provide for network operations support services to CBP and DHS HQ LAN, support to Homeland Security Data Network (HSDN) classified SECRET. The Contractor supports virtual private networking (VPN) solutions and remote access services support, access control, and identity management tasks. The Secondary NSO shall provide equivalent services to support the functions being performed at the Primary NSO. The Contractor shall provide trained, qualified, and cleared staff to support these functions 24x7x365. The Contractor is held accountable for the service level objectives SLOs outlined in Appendix A.

The Contractor roles and responsibilities will include but are not limited too;

- Implementation of approved changes to all policy and enforcement rules on firewalls in response to Secure Internet Gateway change requests
- Troubleshooting and resolution of all firewall related problems
- Alignment with the Security Operations Center to streamline the implementation of network security of the WAN environments
- Network Management Support
- Management and Maintenance of Network Monitoring Tools
- Network Performance Monitoring in a Control Center Environment
- Network Performance Analysis (trend analysis, performance modeling, and capacity planning)
- Proactive analysis of network traffic
- Network Configuration Control & Management
- Network Management (Utilization and Capacity)
- Network Utilization and Availability Reports

- Enterprise Services Management and Monitoring
- Oversight of Managed Service Providers
- Technical Requirements Analysis
- Performance Management
- Mitigation and resolution the detected issues
- Oversight of Managed Service Provider (MSP) SLOs/SLAs
- Tracking “chronic” or recurring problems to escalate within the MSPs Management Chain
- Current network switch and router configurations
- Network Tools Engineering Support
- Evaluation of new tools for proactive monitoring of network performance
- Management and Administration of Network Monitoring Tools
- Operational management responsibility of all IP address assignments
- Tier III IP support
- Accurately documented IP configurations
- Quality assurance on vendor installed routers
- Information Technology Security Support
- Management and Administrative Support
- Service Level Agreements (SLAs)
- Maintaining network equipment (Switches, Routers, Encryptors, Firewalls, etc.)
- Data Collection and Integrity Management of Asset Database(s)
- Network system support (engineer, install, test, maintain, monitor and tune)
- Responding to Tickets forwarded from other responsibility areas.
- Documenting status in the Remedy Trouble Ticket System
- Concept identification
- Requirements definition
- Monitoring and tuning of systems
- Troubleshooting and maintaining systems
- Diagnosing problems before and after occurrence
- Implementing new technology
- Preparing and maintaining documentation in support of the DHS NSO mission
- Voice over IP (VOIP) Engineering Expertise

### **3.3 Technology Service Desk**

The contractor shall provide telephonic support for CBP and its customers. The contractor shall open incident or service request records in Remedy for all calls, faxes, emails, voice mails, and monitored systems. The contractor shall answer all calls received within the Technology Service Desk, (TSD) within 120 seconds, emails within 1 hour, and voice mails within 1 hour, from time each one is received.

The contractor shall maintain and monitor all incident records within Remedy and provide assistance in their resolution when reviewing incident records. This review of open incident or service requests will be conducted on a daily basis and escalate to the proper group and updated

to reflect who was contacted and working the Remedy record. The contractor will review incident records and service request within their Remedy queues every 45 minutes. The contractor shall be responsible for providing customer-focused telephony service support, incident/problem recording, resolution and/or routing problems to the next level of technical support whether they are incoming calls, faxes, emails, reports or automated alert system notifications. If incident requests are unable to be resolved by the Tier One, the Remedy incident record is routed to the appropriate specialist for further technical assistance by warm transfer or SLA requirement. All work performed for each Remedy record will be updated with, what was done to resolve the record, and if not resolved, who was contacted and is working the incident record now.

It is CBP's intention to acquire services that can provide responsive technical support in a manner that meets the ever changing requirements and workload of both CBP and its customers. Therefore the contractor shall research, evaluate, develop, review and implement operational processes and procedures relating to the various support areas under the scope of this task, as required.

The Contract Holder will provide skilled telephonic bilingual customer support for Automated Commercial Environment (ACE) modernization. As the ACE project continues to bring new capabilities to CBP and the trade community, effective communication about this modernization is critical. The ACE Ambassador Program was created in response to the growing interest and requests for more information about ACE and its Modernization program. ACE Tier I Technology Support (TSD) personnel are to offer on-site remote customer systems and application support; to resolve customer problems primarily, but not limited to, the ACE, which will require fluent bilingual knowledge oral and written communication skills primarily (but not limited to) Spanish and French:

- Single 24X7X365 Point-Of-Contact for all CBP incoming requests (phone/email/fax)
- The Contract Holder will provide customer/technical support personnel capable of resolving common and repeatable problems reported by the public, CBP partner organizations, inspections, enrollment centers, Canadian Officials, and CBP customer community.
- Provide support to Trade/PGA and Internal ACE Users.
- Offer Bi-Lingual (Spanish and French) support to Trade 24X7X365.
- Resolve issues if possible within 10 minute timeframe, and direct unresolved tickets on to the appropriate Tiers of support.
- Take steps associated with each Priority and end-to-end problem management/tracking through resolution for Priority 1 and Priority 2 Remedy records.
- Actively Participate on Priority 1 and Priority 2 bridge calls.

- Participate on Root Cause Analyses (RCA) calls, when this requirement does not conflict with incoming call volume/wait times.
- Participate on status calls deemed necessary to support day-to-day project activities, when this requirement does not conflict with incoming call volume/wait times.
- Perform hourly tests on the ACE portal in Production and T&C strings.
- Perform additional twice-daily tests on T&C string.
- Perform additional after-maintenance testing on Production environment.
- Maintain Knowledge Database and technical training requirements.
- Participate in planned disaster recovery exercises, where the skill sets of this team are deemed critical to the exercise.
- The Contract Holder will provide Call and Problem Incident Record (i.e. Remedy ticket) queue management by skilled Tier I customer/technical support management and personnel.
- The Contract Holder will create and update in the development and maintenance of Standard Operational Procedures (SOPs), instructional guidelines and/or troubleshooting guidelines for each of the above-mentioned Tier I operational areas of the TSD.
- The Contract Holder will maintain and following CSPO policies and procedures that have been added or updated in the CBPs Knowledge Base System for each of the above-mentioned Tier I operational areas of TSD.
- The Contract Holder will ensure that refresher training is provided to their technical staff to maintain the staffing level of competency allowing technicians time to follow required services in this SOW.
- The Contract Holder will meet, at least weekly, with the Government to discuss their performance and will provide status reports at least on a weekly basis.
- The TS Government manager will meet at least weekly to discuss statistics, with the Contract Holder to review operational performance measures, including but not limited to: incoming information system problem calls as they relate to each TS operational area such as identify call volume, call abandon rate, elapsed time before calls are answered, call duration and duration before call or problem resolution is achieved. Using these statistics, the Contract Holder will determine appropriate resource staffing levels and operational changes needed to best support the evolving operations of TS.
- The Contract Holder will adhere to the CBP System Life Cycle (SLC), CBP Automated Information Systems Security Handbook, and Process Improvement processes and

procedures, when applicable.

- The Contract Holder will record, monitor, manage and update the CBP Incident Record System (i.e. trouble ticket system) for each operational area identified in the scope of work section. The Contract Holder is also responsible for routing and/or escalating “out of scope” operational areas to other internal and/or external support service area providers. Specifically, BPA Holder shall:
  - Work, Resolve and/or Reassign\* Incident Records that are identified as “Urgent” and/or “High” in accordance with the established Incident Record Assignment/Escalation procedures and record updated problem resolution/escalation status at least every 1 to 2 hours. The Contract Holder is responsible for routing and/or escalating to various other internal and/or external support service area providers in accordance with TSD policy.
  - Work, Resolve and/or Reassign\* Incident Records that are identified as “Medium” and/or “Low” in accordance with the established Incident Record Assignment/Escalation procedures. The Contract Holder is responsible for routing and/or escalating to various other internal and/or external support service area providers in accordance with TSD established escalation policy.

(\*) Reassigned Incident Records require assistance from groups other than those within TSD.

- **Work Requests**

The Government Manager will direct the Contract Holder to perform tasks within the scope of this SOW. The Government Task Monitor or Contracting Officer’s Technical Representative (COTR) will issue these tasks and any additional information required by the Contract Holder. Acceptance by the Contract Holder of all Government proposed due dates or a proposal of an alternative due date will be sent by The Contract Holder via electronic mail if issues arise in completing the assigned tasks as well as a explanation of the factors preventing performance with a proposed alternative solution.

- The Contract Holders customer/technical support personnel will create and assist in the development and maintenance of Standard Operational Procedures (SOPs), instructional guidelines and/or troubleshooting guidelines for each operational area.
- The Contract Holders customer/technical support personnel will assist in the documentation maintenance of CBPs Knowledge Base System for each operational area.
- The Contract Holder will ensure current CBP security products are deployed and security procedures are enforced to reduce data vulnerability.
- The Contract Holder will provide customer/technical support personnel who possess

skills necessary to identify, diagnose, define, coordinate, and resolve problems.

- The Contract Holder will provide customer/technical associate will answer incoming calls and create a Incident Call and/or Problem Record with the following information:
    1. Identify and validate customer contact and address information in the Requester Information field and update customer profile if necessary.
    2. Enter a Brief Description.
    3. Describe the Incident in the Description field.
    4. Enter the appropriate Category, Type and Item.
    5. Enter the appropriate Status in the Status field.
    6. Enter the appropriate Priority number in the Priority field based upon established priority level assignment and escalation procedures.
    7. Enter a Solution in the Solutions Tab when resolved or route/escalate to the appropriate assignment group for resolution if necessary based upon established escalation procedures.
  - The Contract Holders customer/technical support personnel will record, monitor, manage and update the CBP Incident Record System (i.e. trouble ticket system) and are also responsible for routing and/or escalating to other internal and/or external support service area providers. Specifically, the Contract Holder will:
    - Work, Resolve and/or Reassign\* Incident Records that are identified as “Urgent” and/or “High” in accordance with the established Incident Record Assignment/Escalation procedures and record updated problem resolution/escalation status at least every 1 to 2 hours. The Contract Holder is responsible for routing and/or escalating to various other internal and/or external support service area providers in accordance with TSD, CBP and external group established escalation policies.
    - Work, Resolve and/or Reassign\* Incident Records that are identified as “Medium” and/or “Low” in accordance with the established TSD Incident Record Assignment groups and escalation procedures. The Contract Holder is responsible for routing and/or escalating to various other internal and/or external support service area providers in accordance with TSD, CBP and external group established escalation policies.
- (\*) Reassigned Incident Records require assistance from groups other than those within TSD.
- The Contract Holders customer/technical support personnel will create and/or assist in the development and maintenance of Standard Operational Procedures (SOPs), instructional guidelines and/or troubleshooting guidelines.

- The Contract Holders customer/technical support personnel will assist in the documentation maintenance of CBPs Knowledge Base System.
- The Contract Holder will support Tier I customer/technical support personnel to offer Password recovery and/or resets.
- The Contract Holder will provide support to TSD Local Property Officer (LPO) and ensure CBP Property Inventory procedures are executed and all equipment is accounted for.

It is CBPs intention to acquire services that can provide responsive customer support in a manner that meets CBPs changing requirements, workload, existing services and constant move towards emerging technologies.

### **3.4 Program and Project Management**

The scope of this task includes the performance of IT project management support activities, project artifact development, as defined by Federal, DHS, or CBP policy, artifact organization and configuration management, and project management support activities consistent with the Project Management Institute (PMI) Project Management principles and Project Management Body of Knowledge (PMBOK). This Statement of Objectives incorporates CBP policies and practices, allowing offerors to propose a solution to currently known requirements. It is expected that projects, related requirements, and resulting objectives will change over the life of this order, impacting IT subject matter knowledge, staffing ratios and workload. Vendors must consider the changing technologies, projects scope and scale in their contracts.

#### **3.4.1 Program and or Project Planning Services**

IT program and/or project planning services include: project integration planning (Scope, Schedule, and Cost Baselines), scope planning and management, resource analysis, planning, and management, schedule development, management and analysis, risk planning, analysis and management, project cost estimation, quality planning and management, and project performance planning. Additionally, the contractor shall support project control, monitoring, and closeout services. Earned value management, project change control, project remediation, and project status reporting must be addressed.

Tasks identified as being within scope are:

- Project integration planning
- Scope planning and definition
- Project resource analysis and planning
- Requirements development, analysis, and documentation

- Project cost planning and analysis - Analyze project controls to determine if financial calculations, processes, procedures, and reports function as planned, meet the needs of CBP ITP, and meet applicable Federal Standards
- Project schedule development, maintenance, and analysis
- Integrated master schedule development, maintenance and analysis
- Risk management activities, planning, and analysis - Identify, analyze and track risks to the development project sufficiently and early enough to allow for timely risk mitigation actions;
- Communications planning
- Performance planning
- Project control & monitoring activities
- Earned value management
- Project change control
- Project configuration management support
- Project problem remediation
- Project lessons learned
- Project closeout activities
- Project QA audits and findings
- Performance analysis
- Knowledge management/technology expertise
- Program/Project Management artifact development
- Project acquisition planning
- Development and organization of project artifacts
- Development of project performance reports
- Support the development of system component lists and Bill of Materials

- Review and evaluate development technical architecture and system development activities for consistency with DHS and Government standards
- Support Stage Gate Reviews that are required by the Systems Life Cycle (SELC) framework by reporting on: 1) quality and completeness of stage deliverables/exit criteria, 2) issues relating to the readiness of system development to enter production environment during Data Center Operational Readiness Reviews (ORR), and 3) risks and quality issues raised during Production Readiness Reviews (PRR), including a "go" or "no go"
- Evaluate the project core system development activities, including but not limited to: Change Management, Configuration Management, Requirements Management (including review, analysis and traceability), Test Management, and Quality Management
- Report on compliance of processes to industry standards (e.g., Capability Maturity Model)
- Report deficiencies and evaluate changes made to the system, until adequately addressed
- Perform risk and maintainability assessment in each SELC stage to ensure all risk and applicable maintenance activities are planned for and / or in place
- The Contractor select will not perform the role of Information Systems Security Officer (ISSO), however, the Contractor select shall provide IT system security support including the following tasks:
  - Evaluate and contribute to the development of security risk assessments and review resulting Corrective Action Plans
  - Evaluate, contribute to, and monitor security deliverables such as Security Plan Analysis, System Risk Assessment, Business Continuity Plan Analysis, System Rules of Behavior Analysis, and Implementation Plan Analysis
  - Assist in the preparation of project systems for certification and accreditation
  - Support develop of the security assessment plan that includes a complete assessment of all security controls in the information system
  - Review and provide comments to improve Certification and Accreditation project plans, security test and evaluation plans, and security documentation
- Develop action plans for accomplishing risk mitigation activities based upon government-established priorities. Risk mitigation work packages represent logical groupings of security initiatives and consist of the following:
- Coordinate system and application testing activities

- Coordinate and support project meetings
- Monitor and observe development testing activities from unit testing through integration testing
- Program Quality Assurance and Enterprise Quality Management support - the Contractor select shall provide personnel, resources, tools, and facilities, as appropriate, to provide efficient and cost effective program quality assurance support on specific task objectives. Specific tasks may include:
  - Evaluate performed processes, work products, and services against the applicable process descriptions, regulations, standards and procedures
  - Review and evaluate development technical architecture and system development activities for consistency with standards
  - Identify, analyze and track risks to enterprise quality processes sufficiently and early enough to allow the Government to take timely risk mitigation actions

#### **3.4.1.1 Integrated Schedule Requirements**

To complement ITPs program management analysis and planning capability, an integrated schedule of its independent projects is needed. Integrated program schedule support includes:

- Facilitation of requirements gathering and collaboration across ITP to define and develop master schedule requirements
- Develop, baseline and maintain a consolidated and integrated master schedule of ITP project tasks to provide ITP with a “global view” of ITP portfolio activities occurring across the CBP enterprise
- Minimize the amount of manual data entry needed to maintain the integrated program schedule. It is preferable that the schedule to be linked to and dynamically updated when individual project schedules are revised. The applicable project support teams will maintain individual project schedules
- Identify areas of project task commonality, interdependencies, and opportunities for streamlining to improve program efficiency. For example, where multiple projects are planning implementations at common sites, those implementation activities should be merged to minimize resource requirements, time, and/or expenditures. On a weekly basis, the Contractor shall analyze the master schedule and report on potential cross project efficiencies. The Master Scheduler shall collaborate with Project Managers to plan for and realize potential cross project efficiencies.
- Maximize DHS and CBP stakeholder visibility to the integrated ITP program schedule while also assuring maximized security and configuration management of the file.

- Facilitate weekly integrated program schedule review and coordinate meetings with applicable ITP project stakeholders to communicate, coordinate, monitor, and control the integration of evolving project tasks.
- Develop and implement a process for integrating emerging project activities into the integrated program schedule

### **3.4.2 IT Investment Management**

The Contractor select shall provide support services for ITPs enterprise-wide program/portfolio planning. Examples include: IT project cost estimating, cost/benefit analysis, net present value analysis, alternative analysis, and Office of Management & Budget (OMB) Exhibit 300 Preparation & Evaluation.

Some tasks identified as being within scope are:

- Project Cost Estimating
- Cost/Benefit Analysis
- Net Present Value Analysis
- Alternatives Analysis
- Business Case Analysis
- Portfolio Management, Control, & Operational Analysis

## **4 APPLICABLE DOCUMENTS**

Specific DHS/CBP generated documents are for official use only (FOUO). All FOUO documents will be made available for viewing, but shall not leave CBP facilities, photocopied, or pen copied verbatim while viewing. All individuals will be monitored by a CBP representative while viewing the documents. Additional Government Furnished Information (GFI) will be provided to the selected vendor on an "as needed basis" in support of the tasks and activities under this effort.

- Homeland Security Acquisition Regulation (HSAR)<http://www.dhs.gov/xlibrary/assets/opnbiz/cpo-acquisition-regulation-0606.pdf>
- OMB Memorandum M-07-11 "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems"

Vendor's can obtain the following references by requesting in writing from the Contracting Officer's Technical Representative. See Appendix A for DHS CBP Applicable Policies and Procedures.

- CBP Information Systems Security Policies and Procedures Handbook 1400-05C Version 2.1 of October 18, 2006.

- Information Technology Outage Notification Procedure - Field Support Procedure Version 1 of February 26, 2008
- CBP Emergency Preparedness Program 5290-010B of June 8, 2007

Due to the number of Standard Operating Procedures, Vendor's can obtain a list and/or procedures by requesting in writing from the Contracting Officer's Technical Representative.

## **5 PERFORMANCE REQUIREMENTS**

### **5.1 Information Technology Field Services Support**

#### **5.1.1 TECHNICAL PERFORMANCE REQUIREMENTS**

The following technical support tasks shall be required for this effort:

- Task 1: Systems Management Support
- Task 2: Customer Service Support
- Task 3: Resource Management Support
- Task 4: WAN/LAN Support
- Task 5: First Responder Support
- Task 6: Telecommunications Support
- Task 7: Facilities/Modernization Information Technology Infrastructure Support
- Task 8: Project Management Support and Deployment
- Task 9: International Support
- Task 10: Optional Level of Effort Support
- Task 11: Program Management and Administrative Services

##### **5.1.1.1 TASK 1: System Management Support**

The purpose of this task is to ensure that the full range of systems management support is provided. This includes:

- 5.1.1.1 Desktop Support,
- 5.1.1.2 Server Operations Support,
- 5.1.1.3 Systems Security Support,
- 5.1.1.4 Microsoft Exchange Support,
- 5.1.1.5 Software Library Support,
- 5.1.1.6 Database Administration,
- 5.1.1.7 Centralized Help Desk support, and
- 5.1.1.8 Support Information Technology Outages according to policy/procedure. CBP local policies and standard operating procedures are in place and should be followed or revised, as recommended, to best meet the performance objectives of these services. The Government shall be provided an opportunity to review and approve all recommended changes to local procedures prior to implementation

##### **5.1.1.1.1 Desktop Support**

- In providing this support, the Contractor shall:

- Install, repair, configure, and test hardware and peripherals on all incoming computer equipment.
- Respond to end-user software and hardware trouble calls. The contractor shall document all trouble calls utilizing the CBP help system (Remedy).
- Test and document all failed desktop computer systems and hardware and replace such systems and hardware as required.
- Complete hardware and software installations.
- Perform user account management.
- Take all necessary precautions to avoid losing customers data and restore any lost customer data from backups.
- Support office moves which include moving computers, monitors, phones, peripherals, updating inventory and restoring equipment to an operational condition.
- Provide remote site support.
- Provide support for all printers, PDA's, scanners, thumb drives and remote mail devices as approved and used within CBP
- Respond to end-user voice communications trouble calls.
- Provide assistance on normal operating functions of the phone and troubleshoot fundamental connectivity and operational conditions.
- Provide support for remote access hardware and software, and all approved end-user devices.

#### **5.1.1.1.2 Server Operations Support**

The Contractor shall interface with the CBP Helpdesk on issues on all CBP servers to include, but not limited to Exchange, Active Directory (AD), Novell Directory Services (NDS), Domain Controller (DM), Microsoft servers, WINS, DNS, DHCP, systems. In performing this service, the Contractor shall:

- Maintain all systems servers including hardware and software. Servers supported include but are not limited to: file, print, web technology, SharePoint application, and other servers as required.
- Maintain the data backup systems and devices.
- Maintain the data backup media, including onsite and offsite storage.
- Maintain a log identifying media, date of backup, data contained within backup and the location of the media.
- Monitor server system performance and recommend changes in writing.
- Record, in an electronically maintained log, all configuration changes for each system and records of all updates.
- Maintain and document disaster recovery procedures.
- Review all system, security, and application logs for all servers and resolve erroneous conditions.
- Manage disk space utilization on all servers including monitoring and enforcement of pre-determined user quota limits.
- Support antivirus software for the workstations.
- Validate server patch management including installation.
- Install, test and manage software add-ins and hardware devices within the Server environment.

- Coordinate server and technical support for CBP High Security Digital Network (HSDN) specialized applications.
- Travel to, or remotely access, CBP sites to troubleshoot and repair servers.
- Provide Tier 1 and Tier 2 LAN support.
- Provide reports, via government recommended media, on request showing site status.

#### **5.1.1.1.3 Systems Security Support**

At a minimum and to ensure an on-going secure systems environment, the Contractor shall:

- Assist the customer with completing the application to test and integrate non-standard software packages.
- Monitor desktop performance and recommend changes in writing as technology changes.
- Maintain and document disaster recovery procedures.
- Maintain anti-virus protection software.
- Provide workstation anti-virus installation support.
- Generate and review “Workstation” and “Server Patch Management” reports and resolve any discrepancies.
- Manage Active Directory policies, scripts and permissions.
- Interface with the CBP Helpdesk for support of DNS WINS and Proxy.
- Report all suspicious activity to the CBP Computer System Incident Response Center (CSIRC).
- Install, configure and maintain a centralized workstation management tool to track hardware and software inventory, remotely connect to workstations and deploy required software.
- Support web interfaces accessed by the user community.
- Participate in new hardware and software compatibility and usability testing.
- Participate in security audits and assessments.
- Remediate audit findings.
- Participate in Continuity of Operations Plans (COOP) exercises

#### **5.1.1.1.4 Microsoft Exchange Support**

In providing this support, the Contractor shall:

- Interface with the CBP Helpdesk regarding the Exchange Mail Systems.
- Manage database space utilization on all Exchange servers according to CBP policy.
- Install Exchange related antivirus software and provided support of the software. The Contractor shall provide monthly a report of activity of the software in accordance with the deliverable section of this document.
- Provide Exchange Patch Management that includes installation and technical support.
- Manage and support public folder creations/deletions, permission updates and replication.
- Configure and enforce storage limits on mailboxes and public folders.
- Create and delete accounts on mailboxes and custom recipients.
- Interface with the CBP Helpdesk to create and manage distribution lists and group mailboxes.

#### **5.1.1.1.5 Software Library Support**

In providing this support, the Contractor shall:

- Maintain software and license inventory of all systems located at their assigned sites.
- Duplicate CDs used for workstation image loading, remote access and Enterprise agreement software for product development while maintaining an inventory of the master disks.
- Manage user groups for the use of specific software products.
- Destroy all discontinued software in accordance with applicable CBP policy.
- Maintain a record of all discontinued and discarded software.

#### **5.1.1.1.6 Database Administration Support**

In providing this support, the Contractor shall:

- Provide Database Administration support for approved databases that are locally fielded.
- Provide installation and support for Database Patch Management.

#### **5.1.1.1.7 Centralized Help Desk Support**

In providing this support, the Contractor shall:

- Answer customer placed phone calls and inquiries, and record all requests for assistance within the CBP Help System (Remedy).
- Monitor the CBP Help System queue for customer requests for service or assistance. The Contractor shall enter all requests into the CBP Help System.
- Monitor the CBP Help System queue tickets for timeliness of response and completion.
- Review and analyze trouble tickets submitted through the Remedy system and determine their likely reasons, repair times and other relevant information to determine trends and suggest solutions.
- Escalate all calls relating to any system wide outage, such as loss of mail capability, loss of Internet access, or any interruption that is deemed to be beyond a loss-of-service for individual users.

#### **5.1.1.1.8 Support Information Technology Outages**

In performance of this effort, the Contractor is expected to follow the procedures outlined in the "Information Technology Outage Notification Procedures" in responding to Information Technology outages. An outage is defined as an unplanned interruption that halts the delivery of services and may be categorized as Serious, Critical, or Catastrophic.

##### **5.1.1.1.8.1 Serious Outage**

A **Serious outage** is defined as one that affects more than one user, but the circuit remains active; passenger; cargo and illegal alien process is operational; and there are no life and safety issues. When a **serious outage** occurs, the Contractor shall:

- Begin troubleshooting immediately and report to status to their Field Technology Supervisor, if the outage occurs during normal working hours.
- Be expected to respond in one hour of notification of required assistance from their Field Technology Supervisor, if the outage occurs after normal working hours.

#### **5.1.1.1.8.2 Critical Outage**

A **Critical outage** is defined as one that results in loss of communication to a site; an application outage that halts passenger, cargo or illegal alien process; and/or presents a life and safety issue.

When a **critical outage occurs**, the Contractor shall:

- Immediately notify their Field Technology Supervisor, if the outage occurs during normal working hours, and begin to assess whether the outage can be repaired on-site within 15 minutes.
- Contact the National Data Center staff for assistance if the repair cannot be made within 15 minutes.
- Be expected to respond within 15 minutes and no longer than 1 hour of notification by their Field Technology Supervisor if they will be required to respond, if the outage occurs after normal working hours.
- Utilize any available communication method (i.e. cell phone), while en-route, to begin troubleshooting and to assess whether the outage can be repaired on-site within 15 minutes or additional assistance is required.
- Contact the National Data Center during a Critical outage staff for assistance if the repair cannot be made within 15 minutes.
- Continually provide updates to their Field Technology Supervisor until the outage is resolved.
- 

#### **5.1.1.1.8.3 Catastrophic Outage**

A **catastrophic outage** is defined as a sudden and total infrastructure outage (city buildings and/or city-wide telecommunications are down) as a result of a national disaster or act of terrorism. When a **catastrophic outage**, occurs the Contractor shall follow procedures in the Office of Information and Technology Incident Management Plan when responding to catastrophic outages.

### **5.1.1.2 TASK 2: Customer Service Support**

The Contractor shall provide a full range of technology support to customers as it specifically relates to the following sub tasking areas:

- 5.1.2.1 Information Technology Support,
- 5.1.2.2 Visual Information Support desktop computer imaging,
- 5.1.2.3 Web Technology Support,
- 5.1.2.4 Audiovisual and Video Teleconferencing Support, and
- 5.1.2.5 Desktop Training Support.

Local policies and standard operating procedures are in place and shall be followed, or revised, to best meet the performance objectives. The Government shall be provided an opportunity to review and approve changes to local procedures.

#### **5.1.1.2.1 Information Technology Support**

The purpose of this subtask is to ensure that the following information technology assistance is provided. Specifically the Contractor shall:

- Assist users with access and operation of unique systems which are not available on an individual basis. These include specialized applications, software and hardware.

- Manage the use of shared resources to include, desktop systems, scanners, printers, CD-ROMs and digital cameras.
- Provide walk-in support for approved applications.
- Assist walk-in customers with using non-standard peripherals and hardware including scanners, CD/DVD duplication, slide scanners, slide makers, all types of removable media and video capturing.
- Provide end user support for all software loaded on CBP equipment.
- Maintain product information and technical publications on information technology equipment, software, and services.
- Provide conversion capabilities for word processing, spreadsheets, and data files.
- Provide conversion between different media types, size and formats. And provide color printouts and electronic slide presentations.
- Provide email, telephone, and walk-in support to end users of Commercial off the Shelf (COTS) office automation applications.
- Provide support for graphics applications to include, Adobe, Corel and Microsoft.
- Research, evaluate, and test new hardware and software.
- Develop, update, and revise user guides and job aids.
- Provide users with technical solutions to their business and systems needs.
- Contribute to the technical reference library for the support staff and end-users.
- Assist customers with converting video content from one format to another.
- Generate and maintain a standard system image for all desktops and laptops. The image shall be built using the baseline CBP-standard image and contain post-install scripts and modifications necessary only for meeting customer requirements to include and follow established DHS and CBP Security Policy.
- Follow the Federal Desktop Core Configuration (FDCC) guidelines when providing desktop support if the computer is Windows XP or Vista compliant. Refer to the Office of Management directive identified in the “Applicable Documents,” Section 1.4.

#### **5.1.1.2.2 Visual Information Support**

The purpose of this subtask is to ensure visual information support and assistance in the following areas. Specifically, the Contractor shall:

- Assist customers with creating, editing and producing digital video content by providing personal instruction in the use of video systems.
- Assist customers with converting video content from one format to another.
- Create, edit and produce digital video content for customers.
- Develop and maintain a library of digital video content and design elements for customer use.
- Research, evaluate and test new methods of creating, editing and producing digital video content.
- Make recommendations to the government for acquiring new video system hardware and software and for improvements to existing video systems and associated customer support processes based on research, evaluation and testing.
- Design and produce 2D and 3D computer and freehand graphic images/layouts for print, web and multimedia applications. Projects shall include design and creation of logos,

illustrations, flyers, web pages, brochures, pamphlets, posters, certificates, newsletters, briefings, slideshows, and various other advertising materials.

- Develop and maintain graphics libraries that are readily available for customer use. The libraries should be well organized, indexed, and easily accessible to customers. Customers should also be able to preview all library images.
- Assist customers with converting graphics files from one format to another.
- Make recommendations to the government for acquiring new computer graphics system hardware and software and for improvements to existing computer graphics systems and associated customer support processes based on research, evaluation and testing.
- Help users scan images.
- Assist customers with designing and producing computer graphic images/layouts by providing personal instruction in the use of computer graphics systems.
- Create and produce customized marketing materials for the OIT Field Support Operations and Maintenance Branch to include video, print and web-based media.

### **5.1.1.2.3 Web Technology Support**

The purpose of this subtask is to provide support and assistance in all aspects of the current and planned web technologies. Specifically, the Contractor shall:

- Provide web development assistance for the customer's intranet sites
- Assist customers with maintaining their respective home pages.
- Develop and publish intranet content for CBP-wide intranet system (e.g. CBP SharePoint).
- Develop and publish intranet content for the CBP intranet systems.
- Research, evaluate and test new methods of hosting, managing and developing intranet web sites and applications.
- Make recommendations to the government for acquiring intranet system hardware and software and for improvements to existing intranet systems and associated customer support processes based on research, evaluation and testing.
- Assist customers with creating, editing and producing web content by providing personal instruction in the use of CBP intranet publishing systems.
- Keep the customer's intranet systems updated with the latest security patches and server software updates.
- Monitor server logs and troubleshoot server problems for the customer's intranet systems. The Contractor shall take corrective measures and document those measures to resolve any errors appearing in the server logs.
- Configure and administer the server software and components on the customer's intranet systems.
- Perform hardware and software upgrades on the customer's intranet systems.
- Manage user access to view and publish content on CBP-wide Intranet systems.
- Manage user access to view and publish content on the customer's intranet systems.
- Monitor server performance on the customer's intranet systems and make any necessary adjustments to the server configuration to ensure optimal performance.
- Ensure availability of the customer's intranet systems during the customer's core business hours.

- Provide the customer's intranet web publishers with web site statistics for web sites hosted on the customers' intranet systems.
- Manage user access to read and write data in customers' intranet system databases.
- Maintain the customer's web applications hosted on the CBP intranet systems.
- Assist customers with configuring new office web applications on the CBP intranet systems and provide suggestions to offices for improving existing web applications on the CBP intranet systems.
- Explore new ways to automate business processes on the CBP intranet and develop web applications to accomplish this. Development of web applications is to include application design, client-side and server-side programming, database construction, security, testing and documentation.
- Periodically review the office web sites on the Headquarters intranet systems and report any non-compliance with Section 508 of the Rehabilitation Act.
- Ensure that all the customer's web sites on the CBP intranet systems are compliant with Section 508 of the Rehabilitation Act.
- Document existing and new web applications on the CBP intranet systems by keeping detailed records of account, data source, connection and contact information for each application.
- Document any adjustments/changes and server performance problems.

#### **5.1.1.2.4 Audiovisual and Video Teleconferencing Support**

The purpose of this subtask is to provide support and assistance in all aspects of the current and planned audiovisual and video teleconferencing aides. Specifically, the Contractor shall:

- Assist customers with the use of audiovisual systems by providing personal instruction in the use of end-user control interfaces and procedures.
- Maintain setup, monitor, troubleshoot and coordinate the repair of audiovisual equipment for customers.
- Assist customers with the use of video conferencing systems by providing personal instruction in the use of end-user control interfaces and procedures.
- Maintain setup, troubleshoot and coordinate the repair of video teleconferencing equipment.
- Test and verify proper operation of video conference systems.
- Provide on-site audiovisual equipment setup and support for the customer.
- Assist the customer with maintaining an inventory of all audiovisual and video conferencing equipment.
- Maintain a CBP video conferencing contact list.
- Install and configure new audiovisual and video conferencing equipment purchased by the customer.
- Research, evaluate and test new methods of providing audiovisual and video conferencing services.
- Make recommendations for acquiring audiovisual and video conferencing system hardware and software and for improvements to existing audiovisual and video conferencing systems.

#### **5.1.1.2.5 Desktop Training Support**

The purpose of this subtask is to provide support and assistance in all aspects of training. Specifically, the Contractor shall:

- Install, configure, and maintain training facility computers, monitors, projectors, printers and related equipment.
- Assist customers using self-training methods.
- Assist customers using office automation tools.
- Provide one-on-one user assistance.
- Provide user support for office automation applications.
- Assist in setting up temporary, or mobile, classroom environments consisting of laptops and network connectivity to be used in CBP conference rooms or other appropriate locations for CBP developed applications training.

### **5.1.1.3 TASK 3: Resource Management Support**

The purpose of this task is to ensure assistance and support is provided to the customer in the following sub tasking areas:

- 1.5.3.1 Asset Management Support, and
- 1.5.3.2 Disposal of Excess Equipment.

The Contractor shall, following all CBP and DHS policies, research and provide information to satisfy data calls, requests for information and risk assessments.

#### **5.1.1.3.1 Asset Management Support**

The Contractor shall:

- Ensure all computer equipment is properly bar-coded and entered into the CBP inventory management system. The Contractor shall track location, office and user assignments of all inventoried IT equipment.
- Coordinate with the CBP Local Property Officer (LPO) any equipment adds, moves, or changes.
- Conduct annual physical inventories of all computer equipment and individual components located at CBP locations and supported outside agencies.
- Provide a liaison for all maintenance contracts and repairs on IT equipment at CBP locations and supported outside agencies.
- Coordinate with other CBP offices and outside agencies for replacement of defective and/or out of warranty equipment.
- Clearly identify all stand-alone systems.
- Count, track and maintain a database of all spare IT equipment.
- Maintain all spare IT equipment in a ready to issue state.
- Receive, document, unpack, configure and install equipment.

#### **5.1.1.3.2 Disposal of Excess Equipment**

The Contractor shall:

- Maintain readiness to process excess equipment
- Scrub data from hard drives contained in excess equipment.
- Assist in preparing items for shipment.
- Assist in preparing documents to excess property.

#### **5.1.1.4 TASK 4: Wide Area Network (WAN)/Local Area Network (LAN) Support**

The purpose of this task is to ensure that a full range of support services are provided to maintain the Wide Area Network (WAN) and the Local Area Network (LAN).

##### **5.1.1.4.1 WAN Support**

The Contractor shall interface with the CBP Helpdesk to provide the following WAN support services. In performance of these services, the Contractor shall:

- Perform diagnostic testing among LAN components and between LAN and WAN components.
- Install, configure and maintain routers and switches per established CBP policies and procedures as required or directed.
- Facilitate the installation, troubleshooting, and repair of communications lines, data circuits, wireless, microwave, and satellite systems.
- Troubleshoot end-user SSH, HTTP, and other session connection problems.
- Install, label, maintain, and troubleshoot internal network wiring and fiber optic cabling.
- Configure, maintain, and troubleshoot TCP/IP and other network protocols.
- Identify existing potential network problems and report outages with corrective actions.
- Work with remote CBP sites to establish and maintain WAN connectivity.
- Coordinate with remote CBP sites to recover and restore WAN connectivity in case of an outage.
- Coordinate with the Network Architecture and Engineering Group to submit a request based on OIT processes, to determine bandwidth requirements for new and existing facilities.
- Submit documentation to create telecommunications service requests for new networking jacks and cabling lines.
- Follow outage procedures outlined in Task 1, Section 5.1.1.8 of this document during WAN outages.

##### **5.1.1.4.2 LAN Support**

The Contractor shall provide the following LAN support services:

Submit telecommunications service requests for new networking jacks and cabling lines.

- Monitor LAN performance and make LAN upgrade recommendations using management/monitoring software.
- Perform diagnostic testing between network components.
- Recommend configuration changes and network upgrades.
- Install, configure, troubleshoot, and maintain network and network monitoring software (such as Solar Winds, etc.) and hardware, as required or directed.
- Install and configure network protocol software (e.g. TCP/IP).
- Install, configure, troubleshoot, and maintain LANs using CBP approved operating systems.
- Install and configure Layer 3 switches.
- Install, configure and maintain switches and routers.
- Install, configure and maintain network monitoring server(s).

- Install, test, and activate copper and fiber optic LAN cabling.
- Troubleshoot and repair LAN lines.
- Troubleshoot and resolve network issues and problems.
- Document all existing and potential network problems and their corrective actions.
- Document and coordinate with the CBP Helpdesk and/or the NSO the assignment of static IP addresses.
- Generate network diagrams, rack elevations and documentation as requested by the Government.
- Configure, maintain and troubleshoot protocol suite for protocol networks.
- Document LAN issues and problems into the CBP Help system.
- Configure and maintain Novell, Windows and Unix/Linux server configuration and maintenance.
- Respond to all Remedy requests within 30 minutes during normal business hours and in a professional manner.
- Maintain network diagrams, rack elevations and documentation.
- Maintain LAN wiring plant diagrams and floor plan.
- Maintain line diagrams of network connections.
- Maintain equipment logs for core switches.
- Recommend configuration changes and network upgrades.
- Travel, as required or directed, to or remotely access CBP sites and worldwide to troubleshoot and repair LANs.
- Install, configure, and maintain remote access devices and software.
- Report statistical data as requested on LAN utilization.
- Diagram, document, configure and maintain VLANs.
- Report, document, and reestablish connectivity as a result of network outages.
- Reestablish network connectivity for users during office moves.
- Analyze hardware power requirements.
- Perform periodic preventive maintenance.
- Participate in design reviews for new facility or renovation plans.
- Diagram, document, configure and install VLANs in a requested format as requested by the Government.
- Analyze hardware power requirements as well as HVAC affects prior to upgrades and new equipment installs.
- Maintain security of LAN rooms by following documented DHS and CBP security standards.

#### **5.1.1.5 TASK 5: First Responders Support.**

First Responders are volunteer government and contractors who respond to regional or national disasters or emergency situations to restore CBP IT and communication infrastructure.

##### **5.1.1.5.1 General Requirements**

In support of this task, the Contractor shall:

- Shall respond and assist in all First Responders activity.

- Shall be recalled based on their location and/or situation and may be mobilized for extended periods of time.
- Complete all online training as found on the First Support SharePoint site prior to being recalled.
- Be issued by the Government a First Responder safety vest and other items required by all First Responders.
- Recalled based on each situation and may be required to perform their duties in hazardous conditions. The overall responsibilities include the evaluation and restoration of CBP Information Technology systems and to ensure restoration of CBP users to normal operations.

#### **5.1.1.5.2 Systems Management Support**

As required and directed by the on-site Field Support First Responder Officer in Charge, the Contractor First Responders shall perform Systems Management Support tasks as found in Task Section 1.5.1 of this document.

#### **5.1.1.5.3 IT Customer Service Support**

As required and directed by the on-site Field Support First Responder Officer in Charge, the Contractor First Responders shall perform IT Customer Service Support tasks as found in Task Section 1.5.2 of this document.

#### **5.1.1.5.4 Resource Management Support**

As required and directed by the on-site Field Support First Responder Officer in Charge, the Contractor First Responders shall perform Resource Management Support tasks as found in Task 3, Section 1.5.3 of this document

#### **5.1.1.5.5 WAN/LAN Support**

As required and directed by the on-site Field Support First Responder Officer in Charge, the Contractor First Responders shall perform WAN/LAN Support tasks as found in Task 4, Section 1.5.4 of this document

#### **5.1.1.6 TASK 6: Telecommunication Support**

The Contractor shall perform high-level telecommunications engineering support for telecommunications projects, including analysis and integration of products and technology into Customs and Border Protection infrastructures. In performance of this effort, the Contractor shall:

- Draft initial work statements for review.
- Recommend products, technology, and service providers for supporting computer telephone integration (CTI), computer telephony (CT) Voice Over Internet Protocol (VOIP), and telecommunications integration requirements for voice and data networks and skilled in VOIP installation, configuration, maintenance, and troubleshooting.
- Minimize CTI, CT and VOIP integration risks including testing and acceptance plans, quality control processes, and project/task.

- Produce reports as needed such as: call detail reports based on usage, type of calls, minutes or hours of calls, information on incoming or outgoing calls, cost of calls, etc. any parameter that the system allows within two days of notification or request.
- Be certified and proficient in the operation and maintenance of the CBP Phone Systems and shall be responsible for managing, updating and making changes to the system. The Contractor shall update the software as needed.
- Maintain the system installation and integration of CBP VOIP systems. The Contractor shall provide new additions, moves, and changes to the system. The Contractor shall update the software as needed.
- Provide new additions, moves, and changes to the redundant servers that support the CBP systems. The Contractor shall update the software as needed.
- Provide new additions, moves, and changes to the redundant servers that support the CBP VOIP systems. The Contractor shall update the software as needed.
- Perform detailed project management of the installation of required new additions to the telecommunications and IT infrastructures.
- Ensure that vendor supplied telecommunications hardware, software, and installation services conform to applicable work statement and specifications for new equipment and can be maintained as part of the standard CBP operations environment.

#### **5.1.1.7 TASK 7: Facilities/Modernization Information Technology Infrastructure Support**

The purpose of this task is to ensure that the full range of systems management support is provided. This includes:

- 5.1.1.7.1 Server Engineering Support,
- 5.1.1.7.2 Systems Security Support,
- 5.1.1.7.3 Directory Services Support,
- 5.1.1.7.4 Engineering Support, and
- 5.1.1.7.5 Information Technology Outages Support
- 5.1.1.7.6 Outlook and Blackberry Support

##### **5.1.1.7.1 Server Engineering Support**

The Contractor shall be the industry expert on issues regarding Exchange, Active Directory (AD), Novell Directory Services (NDS), Domain Controllers (DC), Microsoft Servers, DNS and DHCP systems, as well as other technologies as they develop. In performing this service, the Contractor shall:

- Install and configure all systems servers including hardware and software. Servers supported include but are not limited to: file, print, web technology, SharePoint application, and other servers as required.
- Install and configure the data backup systems and devices.
- Install and configure the data backup media, including onsite and offsite storage.
- Review server system performance as requested by local Field Technology Officer and recommend changes in writing
- Provide a record of changes of all configuration changes for each system and records of all updates.

- Provide guidance on disk space utilization on all servers including monitoring and enforcement of pre-determined user quota limits.
- Install and configure antivirus software for workstations and servers.
- Install and configure server patch management including installation.
- Install, test and manage software add-ins and hardware devices within the Server environment.
- Travel to, or remotely access, CBP sites to troubleshoot and repair servers.
- Provide Tier 2 and Tier 3 LAN support.
- Provide reports, via government recommended media, on request showing site status.

#### **5.1.1.7.2 Systems Security Support**

At a minimum and to ensure an on-going secure systems environment, the Contractor shall:

- Manage directory policies, scripts and permissions.
- Interface with the Network and Security Operations Center (NSO) and Security Operations Center (SOC) for support of DNS WINS and Proxy.
- Report all suspicious activity to the CBP Computer System Incident Response Center (CSIRC).
- Participate in new hardware and software compatibility and usability testing.

#### **5.1.1.7.3 Directory Services Support**

In providing this support, the Contractor shall:

- Interface with Electronic Mail Operations (EMOPS) regarding the mail systems.
- Provide directory services troubleshooting including replication configuration.
- Create and delete accounts and distribution lists within the enterprise directory services.
- Engineering Troubleshooting Support
- In providing this support, the Contractor shall:
- Answer Field Technology Officer (FTO) placed phone calls and inquiries, and record all requests for assistance within the CBP Help System (currently Remedy).
- Monitor the CBP Help System queue for FTO and customer requests for service or assistance. The Contractor shall enter all requests into the CBP Help System.
- Monitor the CBP Help System queue tickets for timeliness of response and completion.
- Review and analyze trouble tickets submitted through the Remedy system and determine their likely reasons, repair times and other relevant information to determine trends and suggest solutions.
- Escalate all calls relating to any system wide outage, such as loss of mail capability, loss of Internet access, or any interruption that is deemed to be beyond a loss-of-service for individual users.
- Provide escalation as required within existing OIT processes and using Remedy, to Network Engineering for additional analysis and resolution as necessary.

#### **5.1.1.7.4 Support Information Technology Outages**

In performance of this effort, the Contractor will assist FTO's, as requested, in any outage as outlined in the "Information Technology Outage Notification Procedures" in responding to Information Technology outages.

#### **5.1.1.7.5 Outlook and Blackberry Support**

- The contractor shall provide 24 x 7, 365 days per year, Tier 1 and 2 Electronic Messaging Operations support to the TSD in remotely supporting, via the telephone and through other electronic means, the approximately 60,000 plus CBP employees worldwide. The Electronic Messaging Support staff shall be technically skilled in monitoring and resolving problems of Outlook mail infrastructure applications and resolving automated alerts.
- The contractor shall provide 24 x 7, 365 days per year, Tier I and II support to the TSD in supporting local and remote users of wireless electronic messaging technologies such as Blackberries and Palm Pilots. Support will consist of implementing, installing, troubleshooting and resolving problems of CBP standard electronic messaging applications on these devices.
- The contractor shall support the CBP Enterprise Infrastructure Projects Offices (EIPO), specifically the ADEX Project Management Office, in support of the CBP ADEX deployment. The Contractor shall provide project management support as well as technical engineering and operational support. The contractor shall provide on-site resources to perform tasks related to Microsoft Active Directory, Microsoft Exchange engineering and operational functions, project deployment/implementation planning, coordinating and tracking, project documentation creation, documentation change management
- Migration of email across all other mail platforms.
- Prepare documentation in accordance with CBP SDLC, ITIL and CMM best practices, policies, procedures and templates.
- Perform network and system monitoring and provide technical support for application systems and external connections within the defined CBP areas of operation. Monitoring shall be performed predominately through the use of automated system alerts and support system tools.
- Plan, coordinate, perform and document preventative server or system maintenance, software updates, hot fixes, and patches for all CBP Intel based, production servers.
- Develop LAN backup schedule in compliance with CBP electronic data backup/retention policies and procedures. Should no policy or procedures exist, coordinate the development and approval of these procedures. Perform weekly and incremental backups, in accordance with the backup schedule. Restore data from back source(s) as required. Catalog, verify, and store backed up data at off-site storage locations.

### **5.1.1.8 TASK 8: Project Management Support and Deployment**

The Contractor shall provide a full range of project management and deployment support to customers as it specifically relates to the following tasking areas:

- 5.1.8.1 Project Management Support
- 5.1.8.2 Deployment and Implementation Support

#### **5.1.1.8.1 Project Management Support**

The contractor will provide Project Management support and tasks to include but not limited to those listed below.

- Conduct site survey's to assess site needs and readiness to include cabling schematic, network design, electrical power requirement, equipment requirement, and network equipment design.
- Review existing lessons learned documentation from similar past projects when initiating a new project.
- Provide cabling design support; including providing floor plans, layout of equipment, and cabling schematics in formats as requested by the government being either electronic and or written.
- Provide support with gathering cost estimates based on an agreed upon cabling design and all relevant facility documentation.
- Provide feasibility assessments for any project team as requested and provide mitigation options if necessary to support the project.
- Provide technical support and documentation in preparing requests for data communication systems to support new sites, site upgrades, and or relocations. Provide documentation and follow established processes to cancel data circuits when facilities are closed.
- Determine available meeting locations, teleconference bridges, and reserve through available processes. Develop agendas and capture meeting minutes when requested. Distribute announcements, capture and document decisions, issues, action items, resolutions, etc that are identified during meetings in provided formats and templates. Distribute meeting minutes and agenda items in a timely manner as established by the government.
- Maintain the status and provide reports as required by the government, of all tasks involved with multiple concurrent IT Infrastructure projects. This includes progress from initiation through implementation and project close out.
- Facilitate the capturing, and documentation of project lessons learned during a project close out.
- Maintain and organize project artifacts, to include procurement requisitions, delivery orders, site information, bill of materials, points of contact, and copies of certified invoices.
- Participate in project working group meetings.
- Conduct research and recommend appropriate software and hardware design alternatives based upon analysis and projected operational and estimated maintenance support costs.
- Design equipment configurations for each site that reflects user requirements.
- Provide technical support in preparing procurement requisitions for equipment, ensuring proper cost estimates, and that delivery schedules are met in a timely manner.

- Notify appropriate identified field points of contact, based on the project and its location, to advise them of equipment orders, delivery schedules, and planned installation dates.
- Provide pre-installation support in preparing network definitions for all new equipment being installed. This would include such tasks as creating equipment names based on naming conventions, and establishing IP addresses as necessary.
- Maintain location specific information for all sites in a provided and established database. For example, physical and shipping addresses, critical points of contact, hours of operation.
- Provide technical designs with cost estimates to the appropriate project managers, in order to provide the National Finance Centers funding requirements.
- Coordinate with GSA or building owner to properly identify electrical requirements to support equipment, design of computer room/telephone room in according with CBP documented systems security guidelines.
- Provide field based requirements in testing new equipment at the Newington Data Center, ILab, to ensure that equipment is compatible with CBP applications, meets user requirements, and can withstand the various and often extreme environmental requirements in CBP locations.
- If the implementation plan includes a necessary outage, the outage agreement will need to be coordinated by contractor prior to travel.
- The contractor will establish and distribute a day by day breakdown of tasks to be performed onsite.
- The contractor will follow the official CBP change control process. The contractor will request approval by creating a change request based on OIT processes prior to implementations.
- The contractor will create a work breakdown schedule (WBS) on all projects.

#### **5.1.1.8.2 Deployment and Implementation Support**

The contractor will provide Deployment and Implementation support and tasks to include but not limited to those listed below.

- The contractor will be required to propose to the government, a qualified implementation team with available deployment branch staff for project deployments.
- The contractor will be required to travel to domestic and international locations to perform implementations.
- The contractor will document and distribute travel itineraries in accordance with current CBP processes.
- The contractor will manage all facets of onsite implementations to include all tiers of support and will be the target of all escalation during implementation.
- The contractor will provide deployment support to include items listed in Tasks 1.5.1 – 1.5.5.
- The contractor will be required to perform duties during coordinated outage periods to include overnight and weekends as required to not hinder the primary mission of the CBP facility.
- The contractor will provide, on a weekly basis, a report of daily accomplished tasks and statuses of on going projects.

#### **5.1.1.9 TASK 9: International Support**

International covers all International programs intended to help increase security for containerized cargo and foreign passengers traveling to the United States from around the world. This support includes all outlined tasks, Task 1-4, required to install and maintain all OIT equipment and communications.

- All international travel processes will be followed, including but not limited to Country Clearances.

#### **5.1.1.10 TASK 10: Optional Level of Effort (LOE)**

The following refers to an optional level of effort and associated subtasks that CBP may exercise at their discretion. The decision to invoke any of these subtasks shall be based on the level of support that is required, project length and the amount of project funding received.

Examples of expected projects are:

- Western Hemisphere Travel Initiative
- ACE Modernization Information System
- Windows File and Print
- Position Model
- Container Security Initiative

Written notice shall be provided to the Contractor at least twenty (20) working days before start the start of the optional effort.

#### **5.1.1.11 TASK 11: Program Management and Administrative Services**

The Contractor shall provide general administrative support and other direct charge support. Professional services to be performed will include but are not limited to the following:

The Contractor shall provide on-site clerical and administrative support to the ENTS. Tasking will include generating and maintaining of program and project files and database, and preparing and distributing of project reports and supporting documentation.

The Contractor shall also provide facilities and supplies for hosting meeting and conferences; preparing overhead transparencies and slides; printing and copying services; communication services (voice, video, and data) and overnight mail services.

The Contractor shall provide professional support to assist in program management functions, it includes, but not limited to, financial analysis, cost benefit and earned value support, logistics support, training support, and schedule support.

### **5.1.2 TASK ORDER AND CONTRACT MANAGEMENT REQUIREMENTS**

Use of Microsoft Project / Project Server for Reporting Purposes.

- The Contractor shall perform program and project planning and management duties to facilitate the development of the system and operational requirements for the task elements. This will include the preparation of plans and schedules based on technical and

project data; tracking program funds; scheduling and conducting technical and planning meetings; conducting project reviews; and preparing status reports. This includes entering program related information in CBP's Microsoft Project server. The Microsoft Project Server will integrate with WorkLenz to publish project information and schedules for Project Management Reviews.

- The Project Scheduling tool is required to accomplish the following:

Manage CBP/CIO resources both effectively and efficiently from an enterprise-wide standpoint;  
Plan the development of new investments and projects in support of agency goals and objectives;  
Ensure that investment and projects are being managed within specified cost, schedule, and performance parameters;  
Foster the development of effective corrective action plans when needed.

- The Contractor shall be familiar with this tool and enter, track and report associated contract activities, as directed by the Program Office Task Monitors or the COTR, within the Microsoft Project Server tool. The Contractor shall update information at regular one week intervals to provide Senior CBP Management with clarity, insight and visibility into on-going IT projects and operations. If support is required for Microsoft Project server, the Contractor will contact the Program Manager Task Monitors or the COTR directly, and will not attempt to seek support from Microsoft or the licensor directly.

## **5.2 Network and Security Operations Center, DHS OneNet**

### **5.2.1 GENERAL REQUIREMENTS.**

Under the direction of the Government On-Site task monitor (OTM) the contractor shall provide a wide range of Network services to include but not limited to, monitoring and analysis, firewall engineering and administration, switch and router engineering and administration, escalation and reporting, network trouble ticket tracking and mitigation, network engineering and integration. The scope of this effort contains the services estimated necessary to support success.

The service outlined in the objectives and listed in the following Tasks will ensure the Contractor meets all Agency and Department needs while maintaining architecture integration and alignment across the enterprise.

The Contractor shall develop and submit for approval to government standard operating procedures (SOPs), Tactic's Technique's & Procedures (TTPs) and Operating Instructions required to facilitate each task and subtask below.

The contractor shall ensure NSO staff maintains a minimum Department of Defense (DOD) SECRET clearance.

### **5.2.2 Project Management**

The Contractor shall manage activities defined in this SOW, in accordance with project management principles, to include the development and documentation of requirements, project plans, schedules, risk registers, and mitigation strategies.

The Contractor shall conduct reviews with the Contracting Officer, Contracting Officer's Technical Representative (COTR), or designated representative that accurately report cost, schedule, and performance status as measured through an implemented Earned Value Methodology.

The Contractor shall be aggressive in the identification and resolution of risks, issues, and dependencies.

The Contractor shall be proactive in the identification of internal and external dependencies.

The Contractor shall provide weekly status reports on the project progress.

The Contractor shall utilize Tasks to separate new and existing projects and funding sources as requested.

The Contractor shall provide monthly invoices to itemize costs at the project level and within each project by the customer approved Work Breakdown Structure (WBS). Each project shall be provided a Task and at the request and approval of the customer. Invoices shall include a summary Tasks page. Additional Task numbers shall be established for projects or a grouping of activities so that each funding source can be billed accurately.

The Contractor shall provide detailed standard reports and ad hoc reports as requested by the customer. The standard reports shall include the Integrated Master Schedule and Cost Performance Report.

The Contractor shall provide Integrated Baseline Reviews as requested.

#### **5.2.2.1 Constraints**

- Solutions shall be consistent with industry best practices, Department principles, Configuration Management (CM), Technical Reference Model, and System Life Cycle development.
- Solutions must be compliant with the Department Enterprise Architecture directives, OneNet architecture, the Federal Information Security Management Act (FISMA) and other applicable federal, Department security, acquisition, IT, and asset management laws, regulations, rules, and policies.
- Solutions must be compliant with Enterprise Network Engineering Services: Governance Technical Reference Model.
- No Developers shall have access to Production environments.
- All changes to productions must follow the Architecture Review Board (ARB) and Change Management Policy.

### **5.2.2.2 Transition Plan, if applicable**

The contractor must be prepared to support CBP government leads, within the purview of this task order, to provide a 30 day transition period from the incumbent contractor. The required period is for the transition planning or program execution, associated with meeting the agreed to transition timeline, as directed by Government personnel. This includes the following types of taskings:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

### **5.2.2.3 Network and Security Operations Center Support**

#### **5.2.2.3.1 Network Problem Identification, Troubleshooting, and Maintenance**

- The Contractor shall be responsible for identifying, diagnosing, defining, performing, and documenting Tier 2 remedial action taken to resolve network connectivity issues affecting Data Center mainframe, front-end, and client server systems in the production environment. The Contractor shall create a ticket as soon as a condition is detected that has a performance impact on the OneNet Services. The Contractor shall work with the Government to develop a set of guidelines for severity level assignment to a ticket based on service level impact. In the event of a network problem requiring Tier 3 support, the NSO Tier 2 will indicate the presence of network problems through the redistribution of a trouble ticket (via the Remedy Action Request System – the current problem reporting system) to the NSO Tier 3 Network Operational Engineering support responsibility area. The Contractor shall be responsible for troubleshooting OneNet to isolate the source of problems, resolve all network problems, or refer the problems to the appropriate responsibility area. Problems that cannot be resolved at the Tier 3 level will be escalated to the Network Engineering Branch for assistance when all efforts have been exhausted. Network components may include such devices as: cabling, modems, digital/channel service units, concentrators, bridges, routers, switches, firewalls, file servers, link encryption devices, secure frame units, gateways, and protocol converters.
- The Contractor shall continuously monitor the trouble ticket system for new escalated tickets and update at a minimum every hour and when appropriate. All information entered into a ticket shall be clear, concise and accurate. Upon receipt of a trouble ticket, the Contractor shall initiate immediate action to clearly define the problem and effect

immediate resolution, or document the problem in the trouble ticketing system to effectively track it to satisfactory resolution, or redistribute it to the appropriate group of responsibility for action toward satisfactory resolution.

- The Contractor shall determine when analysis of these system components (See first bullet) is necessary based upon diagnostic information provided by approved Government sources, obtained or developed by the Contractor (CiscoWorks, Concord eHealth/LiveHealth, Netcool, NetView, Tivoli, Solar Winds and other distributed processing-oriented management tools). The Contractor may access the network during the course of troubleshooting problems in order to use diagnostic applications resident in the system. In addition, the Contractor shall be responsible for monitoring all network devices using diagnostics application tools currently in place, to include any future additions to the hardware configuration.
- The Contractor shall document each step in the troubleshooting process as it occurs and update the trouble ticket. Due to the complex nature of networks, it is possible for the source of a network problem to reside in one or more devices concurrently. As such, the Contractor shall perform troubleshooting techniques to isolate the source of, diagnose, and resolve or assist in the resolution of network problems.
- The Contractor shall use existing diagnostic tool or tools that are appropriate for use in diagnosing problems. The Contractor should also recommend tools to enhance or replace existing tools.
- The Contractor shall/when required participate and/or lead in conference calls during mitigation actions of network anomalies.
- The Contractor when directed shall provide the government with after action reports regarding troubleshooting efforts and/or resolution actions taken during network event troubleshooting.

#### **5.2.2.3.2 Network Problem Resolution and Referral**

- The Contractor shall refer network problems to various sources when resolution cannot be achieved by Contractor personnel. If diagnosis or resolution has not been completed in accordance with the current established escalation policy, the Contractor shall escalate the problem to higher authority (for example Tier III engineering support) for further action within the Department. Specifically, problems shall be escalated to the Task Monitor and/or Contracting Officer's Technical Representative (COTR).
- The Contractor shall refer problems to equipment vendors when problems are detected in hardware or circuits that are operated, maintained or under vendor warranty. The Government will provide the Contractor with an updated and official list of vendors and the respective hardware/software components and telecommunication lines they service.

#### **5.2.2.3.3 Network Problem Resolution Procedures, Documentation, and Reporting**

- The Contractor shall take appropriate action towards problem status documentation, resolution and prevention as required. The Contractor shall also provide information to impacted users promptly regarding the status of changes, enhancements, and problem resolution. The Contractor shall complete resolution or referral of all network problems as soon as possible after receiving a Trouble Ticket.
- The Contractor shall work with the DHS Steward to develop an acceptable ticket escalation process. Escalation shall occur in a judicious manner and DHS involvement is not necessary to facilitate escalation.
- The Contractor shall manually enter a narrative description in trouble tickets of all information relative to trouble shooting problems to resolution and completion status.
- The Contractor shall ensure that all documentation is clear, concise, and accurate.

#### **5.2.2.3.4 Network Installation Support**

- The Contractor shall install or modify network components and other systems as required. This includes physical and logical connections with switches, routers, firewalls, link encryption devices, and public/private key hardware/software components. No modifications or changes shall be made without an approved change request. The Contractor shall support implementation of configuration management processes and support tracking and reporting of configuration changes. The primary DHS/CBP NSO keeps the configuration of all DHS/CBP site Nodes. The Contractor shall update the configuration into this server once a configuration change is made to a DHS/CBP Node. The Contractor shall work with the DHS OneNet Steward to adhere to the approved process for introducing a scheduled maintenance or network diversity changes.
- The Contractor shall provide support in troubleshooting network problems associated with new or revised hardware or software installations. The Contractor shall provide support in coordinating new off-network connections including direct links with other agencies. The Contractor shall also provide support in resolving or referring connectivity problems that may occur when DHS Component offices are relocated, to include problems resulting from the installation of new off-network links. The Contractor shall update baseline artifacts to include logical design, as-is drawing, and other baseline documents. Occasional staff travel requirements may occur as a result of requirements but is addressed on a case by case basis.
- The Contractor shall provide a list of all newly installed Government owned network equipment for input into an Inventory Management System.

#### **5.2.2.3.5 Network and Security Operations Center Communications Area Equipment Access Control**

- The Government will approve access control to the communications area for Contractor work to be performed on the equipment. The Contractor will maintain and establish access control procedures, checklists, equipment documentation, diagrams, and equipment inventory.

#### **5.2.2.4 NETWORK AND SECURITY OPERATIONS CENTER SUPPORT SERVICES**

##### **5.2.2.4.1 Network Monitoring**

- The Contractor shall provide support to perform proactive and continuous monitoring of the network. Upon detection of such failures, the Contractor shall initiate contact with the Network Service Provider to obtain the problem information necessary for recording and tracking the outage. A System trouble ticket will be generated to reflect the failure and transferred to the managed network services provider for follow-up.
- The Contractor shall be responsible for management notification of all high impact/priority failures using standard operating escalation procedures to ensure that any alternate support groups are notified of the problem, and estimated time of repair.
- The DHS OneNet Steward requires visibility into the Service Providers backbone (e.g., Access, Points of Presence (POP), and IP MPLS network) in order to manage end-to-end DHS/CBP LAN, MAN and WAN performance. The Contractor shall provide a near real-time (in seconds) map of DHS/CBP related access connectivity and status, POP to PE connectivity and status, Provider Edge (PE) Router-to-PE Router connectivity and status, and, bandwidth utilization for DHS/CBP LAN, MAN and WAN traffic and trend analysis.

##### **5.2.2.4.2 Problem Tracking and Escalation**

- The Contractor shall be responsible for tracking all network component failures and effecting escalation actions necessary to ensure appropriate vendor support response and within designated time thresholds established. For serious network degradation, the NSO network management tools will be configured with thresholds that will alert NSO technicians of a potential problem and a trouble ticket has to be generated for tracking and troubleshooting purposes. For high bandwidth utilization the ticket is escalated for further performance and analysis statistics within the NSO. Recommendations are made to the appropriate functional area responsible for taking action to correct the problem such as Network Engineering or Field Support.
- The Contractor shall ensure appropriate information entries are made within the network system trouble tickets. Escalation to the next level vendor and management is performed when resolution thresholds are exceeded.

##### **5.2.2.4.3 Problem Reporting**

- The Contractor shall complete problem status documentation, management problem briefs, and ticket status reports as denoted within applicable support procedures.
- The Contractor shall provide information updates to management and alternate support groups regarding status of problems.
- The Contractor shall interact directly with the managed network services, alternate support vendors and support groups as directed, to provide a single point of accountability and information relative to outages.
- The contractor shall provide daily Network Operations Briefings to enhance the leadership situational awareness of network anomalies and impacts associated with network outages.

### **5.2.2.5 Network Management System Support**

#### **5.2.2.5.1 Network Fault and Performance Monitoring**

- The Contractor shall be responsible for using current management tools to monitor the current network architecture as well as additions and changes to devices and configurations.
- The Contractor shall have access to the use of a wide assortment of management tools to assist in identifying, analyzing and defining network system problems. These tools include, but are not limited to CiscoWorks, Concord eHealth/LiveHealth, Netcool, NetView, Tivoli, Solar Winds, Managed Objects and other distributed processing-oriented management tools.
- The Contractor shall select the management tool or tools that are appropriate for use in monitoring networks and diagnosing problems.

#### **5.2.2.5.2 Network Utilization**

- The Contractor shall be responsible for monitoring network utilization to ensure the network infrastructure accommodates customer traffic, helps reduce operational costs, and establishes a foundation for future services.
- The Contractor shall coordinate with other Department entities and external organizations when required for establishment and verification of baseline and operational network utilization. The utilization statistics shall be captured primarily using available tools to monitor device interfaces in relation to transmission media capabilities.

#### **5.2.2.5.3 Network Availability**

- The Contractor shall monitor network availability and compare sample data with the information in the commercial service provider circuit availability reports for verification and validation of outage statistics.

#### **5.2.2.5.4 Network Trend Analysis**

- The Contractor shall perform network trend analysis to compile daily and/or longer-term reports for various network traffic areas of interest. These reports shall supply both generalized and specific information about targeted areas and shall provide useful snapshots of information. These reports shall include but are not limited to daily and weekly reports covering various error conditions, workload (i.e. CPU and memory), and network utilization. Customized trend analysis reports shall be provided based on current monitoring capabilities with emphasis on tools such as Concord's eHealth.

#### **5.2.2.5.5 Network Capacity Planning**

- The Contractor shall perform data collection to assist in network capacity planning. Network usage and configuration information shall be used with performance statistics to reflect current and long term bandwidth utilization. This information shall be used to

better estimate future requirements based on application, organizational, or technological changes as well as adjustments to provide improved cost/benefit of current resources.

#### **5.2.2.5.6 Network Problem Tracking and Escalation**

- The Contractor shall be responsible for tracking all commercially provided Managed Network Services (MNS) network component failures and effecting escalation actions necessary to ensure appropriate vendor support response within established Service Level Objectives (SLO's) and Service Level Agreements (SLA's).
- The Contractor will ensure appropriate information entries are made within the network system trouble tickets and escalation to next level vendor and management is performed when resolution thresholds are exceeded.

#### **5.2.2.5.7 Network Problem Reports and Documentation**

- The Contractor shall complete problem status documentation, management problem briefs, and ticket status reports as denoted within applicable support procedures.
- The Contractor shall provide information updates to management, alternate support groups and the Department Component Operation Centers regarding status of problems.
- The Contractor shall interact directly with the commercially provided MNS center, alternate support vendors and support groups as directed, to provide a single point of accountability and information relative to outages.
- The Contractor shall provide various reports such as:
  - Network outage reports from daily trouble tickets and compiled into weekly ticket summaries to be added to monthly graphs for comparison of problem types.
  - Measurable goals compiled monthly from the commercial network service provider ticket performance.
  - Chronic network outages compiled monthly from problem reports identifying chronic network issues that require attention.
  - Network outage statistics and/or reports on a case-by-case basis.
- The Contractor shall ensure that all reports and documentation is clear, concise, and accurate.

#### **5.2.2.5.8 Network Quality of Service (QOS)**

- The Contractor shall monitor the network QOS to ensure provisioned services are adequate for specific applications and that they continue to meet customer requirements.

### **5.2.3 Systems Administration**

- The Contractor shall evaluate the capability, performance and capacity of the current system and the associated tools for performing the DHS/CBP NSO functions; and provide a recommendation on the necessary system and tools enhancements or upgrades. If required, the Contractor shall provide the additional necessary systems and tools for upgrading the current DHS/CBP NSO to monitor, manage and resolve troubles associated with DHS/CBP services. The Contractor shall also propose a transition plan and support

the implementation of the proposed systems and tools upgrade for the DHS/CBP NSO consistent with the transition plan.

- The Contractor shall assist in the design and implementation of multi-protocol networks using routers and large bridged networks and creating and maintaining network documentation. Assisting user groups with network and communications issues. Defining of routed networks addressing schemes, designing network links, building and configuring the Internet with IP routers, and segmenting network bridges. Troubleshooting IP configuration operating systems and activating workstations. The Contractor shall be experienced in the support of multi-vendor network systems, solving connectivity problems using major applications, troubleshooting and isolating related problems.
- The Contractor shall implement, install, document and maintain complex or large scale systems software, which may have many modules or inter-relations with other software systems. The Contractor shall have extensive experience in multi-vendor systems software used for network management and monitoring tools.
- The Contractor shall translate data of information into hardware, software, and procedural recommendations. Perform the planning of uninterrupted transition to and staging of implementation to hardware/software procured by the government. Develop and write position papers, planning guides, technical specifications, and user guides. Provide technical leadership and direction on extremely complex systems throughput problems or crucial database software problems as required.

### **5.3 Technology Service Desk**

The scope of this effort contains the services CBP estimates are necessary to support ENTS program success. The contractor may make changes to improve services as long as the impact to any other program is not affected.

The service outlined in the following Tasks will ensure the Contractor meets all Program Offices needs while maintaining architecture integration and alignment across CBP enterprise.

The contractor-operated help desk shall be the primary point of contact/ entry point for all trouble calls for CBP and its customers. This support for CBP and its customers consist of; answering the phone, resolution of tickets when possible, email or fax and creating an incident record or service request in Remedy documenting the record according to support deliverables and supports virtual private networking (VPN) solutions and remote access services support, access control, and identity management tasks.”

- Identify and validate customer contact and address information in the Requester Information field and update user profile if necessary.
- Enter exact but Brief Description of incident
- Describe the Incident in the Description field
- Enter the appropriate Category, Type and Item
- Enter the appropriate Status in the Status field

- Enter the appropriate Priority number in the Priority field based upon the assignment and escalation documentation
- Enter a Solution in the Solutions Tab in accordance with incident resolution.
- Provide problem resolution, referral and escalation as required by CBP procedures.
- All submitted escalation reports shall be clear, concise, and accurate.

### **5.3.1 Support Services**

The Contractor will manage activities defined in this SOW, in accordance with project management principles, to include the development and documentation of requirements, project plans, schedules, risk registers, and mitigation strategies.

### **5.3.2 General Services**

- The Contractor shall be aggressive in the identification and resolution of risks, issues, and dependencies.
- Answer the phone.
- Reduce Wait times for customers on the phone.
- Restore normal service as quickly as possible
- Ensure that incidents and service requests are processed consistently and in the guidelines within this document, CBP's policy and procedures.
- Direct support resources where most needed/ required.
- Provide information that allows all support to processes and reduce the number of incidents.
- Management and planning of the day to days activities to ensure minimal impact to CBP and its customers.
- Acquire qualified Help Desk Manager and staff.
- Gather and analyze statistics on personnel performance, customer satisfaction and making corrections to improve both.
- The Contractor shall provide weekly status reports on the project progress.
- The Contractor shall utilize Contractor Line Item Numbers (CLINs) to separate new and existing projects and funding sources as requested.
- The Contractor shall provide monthly invoices to itemize costs at the project level and within each project by the customer approved Work Breakdown Structure (WBS). Each project shall be provided a CLIN and at the request and approval of the customer. Invoices shall include a summary CLIN page. Additional CLIN numbers shall be established for projects or a grouping of activities so that each funding source can be accurately.
- The Contractor shall provide detailed standard reports and ad hoc reports as requested by the customer. The standard reports shall include the Integrated Master Schedule and Cost Performance Report.
- The Contractor shall be proactive in the identification of internal and external dependencies.
- The Contractor shall provide weekly status reports on the project progress.

- A kick-off meeting with briefing charts will occur no later than 10 working days after award. The deliverable from the kick-off meeting should be the kick-off meeting briefing charts. In said meeting should cover current milestones and dates, status of hiring, status of clearances and the status of their transition of work from the incumbent to contractor. All contractor key personnel should attend the kick-off meeting.
- The Contractor shall provide monthly invoices to itemize costs at the project level and within each project by the customer approved Work Breakdown Structure (WBS). Each project shall be provided a CLIN and at the request and approval of the customer. Invoices shall include a summary CLIN page. Additional CLIN numbers shall be established for projects or a grouping of activities so that each funding source can be billed accurately.
- The Contractor shall provide detailed standard reports and ad hoc reports as requested by the customer. The standard reports shall include the Integrated Master Schedule and Cost Performance Report.
- The Contractor shall provide Integrated Baseline Reviews as requested.

### 5.3.3 Project Support

The contractor shall provide support in the following;

- a. The contractor shall provide phone support and participate in special projects or pilot programs not mentioned in Statement of Work. Special pilot projects not to exceed 500 customers.
- b. The contractor shall participate when required in CBP Disaster Recovery Operational tasks.
- c. The contractor shall ensure that refresher training is provided to their staff on a regular basis to maintain the staff's level of competency.
- d. The contractor shall meet weekly with the government to discuss performance and will provide status reports on all individuals statistics assigned to task.
  - Statistics shall include but not limited to:
    - Total calls offered, Total calls answered
    - Total calls abandon, Total calls transferred
    - Total voicemail calls, Tickets closed with two hours, eight hours, same day, 2<sup>nd</sup> day, Email Incident records opened, calls abandon, elapsed time before calls are answered, call duration and duration before call or problem resolution is achieved. Using these statistics, the contractor shall determine appropriate measures to take to improve statistics and customer satisfaction.

### 5.3.4 Password Services

- Account Creations and Unlocks;
  - The contractor shall provide a professional and technical staff capable of resolving commonly reported problems such as account unlocks and

account creations. These accounts will be but not limited to the following and security requirements are used and followed for each of the following;

- PASSWORD ISSUANCE CONTROL SYSTEM (PICS) system is an automated data processing system that processes and stores sensitive and unclassified information about individuals. This information is covered by the Privacy Act and therefore must be protected against disclosure and tampering. Any loss, misuse, or unauthorized access to this sensitive information could affect national interest, the conduct of federal programs, the privacy to which individuals are entitled under Section 552a, Title 5, U.S. Code, and consequently, sensitive DHS ADP systems.
  - CBP Technical Service Center PICS officers currently have the rights and permissions to change/grant passwords in the PICS system for all Department of Homeland Security users. CBP PICS officers are currently authorized to grant new access for CBP THD personnel only. Upon request, CBP THD PICS officers will verify the identity of requestors and closely adhere to the rules and guidelines regarding PICS access and password resets. All issues that CBP PICS officers are unable to resolve are routed to the Regional PICS officers and Headquarters PICS officers as appropriate.
- The Contractor shall provide a professional and technical staff capable of resolving commonly reported problems in the TECS. TECS client uses this system for performing queries, entering, modifying, and deleting reports or subject records. The team provides answers to general questions that users may have while using the TECS system. The team also supports users with uploading and downloading data and images to and from the TECS database.
- Other Account & Unlock tasks are listed below but not limited to the following:
  - Operating System
  - Mainframe
  - LAN/WAN
  - Domain
  - Active Directory
  - Windows 2000, XP, Vista
  - Applications but not limited to;
  - E-mail password resets
  - Mainframe and its many Applications
  - Not limited to TECS/ACS/Admin Production
  - US Visit \ Arrival
  - Virtual Learning Center VLC
  - External Accounts & Account Unlocks
  - VPN/FOB Accounts
  - CSI Accounts/Unlocks

- Other CBP support applications for internal and external customers

#### **5.4 Program and Project Management**

The Contractor shall address how each project, when initially conceived and authorized, supports CBP strategic objectives and contains acceptable risks regarding the project's objectives: technical, cost and schedule. In addition, the Contractor shall plan, control and lead its programs and projects so that each will achieve its end objective within its intended scope, on schedule and within budget. During the course of its project activities, the Contractor will analyze its project portfolio to determine the optimal mix and sequencing of interrelated project requirements and activities to achieve the most effective and efficient consolidated use of resources, i.e. cost, labor, infrastructure, technology, etc. Where possible, the Contractor shall substantially improve its project artifact timeliness, accuracy, completeness, and currency.

The Contractor staff shall 1) possess and maintain technical competence in project related technologies and, where applicable, professional certification within its areas of responsibility, 2) to develop and deploy innovative, modern and robust technologies and infrastructure that maintains a reliable, stable and secure IT environment 3) to develop and deploy secure systems and advanced technologies to improve targeting and screening of goods, people and conveyances entering the United States and 4) Implement systems and processes to efficiently construct, maintain, distribute and dispose of IT assets needed to carry out the CBP operational missions.

The Contractor shall perform in conformance to requirements of overarching federal, DHS and CBP policy, regulations, guidelines, and mandates applicable to Federal IT capital investments, IT project management, enterprise architecture, and for planning and reporting project performance.

The Contractor shall conduct a non-disruptive transition of ongoing project support activities from the incumbent vendor to the Contractor select upon award of this contract.

##### **5.4.1 Constraints**

Project solutions, support practices, and deliverables shall be consistent with policy and/or guidance referenced below. Referenced versions may change during the performance of this task. The Contractor select shall be responsible for maintaining compliance with policy version changes as applicable.

###### **5.4.1.1 Operational Constraints**

- Development and testing of new or revised technology shall not occur within the CBP IT production environment. Development and production environments shall be separate

###### **5.4.1.1.1 Risk/Issue/Deviation Escalation**

- Issues impacting critical path project tasks shall be reported to the COTR, Task Monitor, and ITP Government Project Lead via email within 2 business hours of their discovery. Escalation information shall include a description, impact, and proposed alternatives

- Upon immediate determination of a 10%+/- deviation for project cost or schedule, provide information updates to the COTR, Task Monitor, and ITP Government Project Lead. Escalation information shall include a description, impact, and proposed alternatives.

## **6 TECHNICAL PERFORMANCE STANDARDS**

### **6.1 Information Technology Field Services Support**

The table below reflects the performance standards that have been established by the Government. The table also indicates the areas in which are most important for the successful performance of this Statement of Work. Although, the government has not established an incentive program, failure of the Contractor to meet these levels shall be reflected in the Contractor's performance evaluation.

Program Service Objective	Required Service	Surveillance Methodology	Performance Standard
Desktop Support - TASK 1: Systems Management Support			
Measures the quality of performance and the responsiveness to user calls that generate IT Service Desk Tickets.	Measure time to respond to user requests via the CBP Help System (Remedy).	Periodic Inspection	<p>Resolution of all service requests within the established SLA, defined by a count of the number of hours required to resolve the incident. Time runs continuously from ticket submittal.</p> <p>Upon completion of an issue, the ticket is marked as Resolved, the Remedy timer is stopped and a notice is sent to the customer. The customer shall be given the option of concurring that the issue is resolved or reopening the issue.</p> <p>The customer shall be given five (5) business days to respond, after which time the ticket may be closed.</p> <p>If the customer does not concur, the ticket is reopened and the Remedy timer resumes. The ticket shall continue to be worked to resolve the customer concerns.</p> <p>Conflicts shall be resolved by the customer POC and the Operations &amp; Maintenance Branch Chief and/or Area Manager, as appropriate.</p>
Measures the customer satisfaction to the	Determine the level of customer satisfaction	Random Intervals	The results of all four quarters shall indicate

Program Service Objective	Required Service	Surveillance Methodology	Performance Standard
Desktop Support - TASK 1: Systems Management Support			
contractor support	as it relates to technical support		<p>an average customer feedback shall be positive. Negative feedback shall be reported to the supervisor. Customer satisfaction surveys shall indicate an overall satisfaction rate of 4 out of a level of 1-5 (5 being exceptional).</p> <p>The satisfaction survey shall be the same across the board - Maximum of number of questions should be 5 - questions would indicate</p> <ol style="list-style-type: none"> <li>1. At what level are you satisfied with the response time to your service requests?</li> <li>2. At what level are you satisfied with the quality of the results of your service requests (are the tickets resolved with the first request)?</li> <li>3. How satisfied are you with the reliability of your network connectivity?</li> <li>4. How satisfied are you with the reliability of your computer equipment or peripherals?</li> </ol>

Server Operations Support TASK 1: Systems Management Support			
Measure the time it takes to restore server availability to the network.	Measure the time to restore network connectivity.	100% of related tickets	The contractor shall restore normal file server operations /connectivity less then 4 hours.  If the server requires re-imaging the timeframe should not exceed 28 hrs
Measures the availability of the CBP managed file and print servers.	Measure the percentage of time the file and print infrastructure is available during the period	Periodic Inspection	File and Print Infrastructure availability $\geq 99.99\%$
Measure File and Print Services Response Time	Measure the response time of the CBP managed File and Print Services	Periodic Inspection	Average File Server response time $\leq 5$ seconds  Average Print Server response time $\leq 30$ seconds
Systems Security TASK 1: Systems Management Support			
Measure response to system security violation reported by user to ensure system security per CIS HB-1400-05C, p28-29.	Measure time to respond to reported security incidents via the CBP Help System (Remedy), email, or phone.	Periodic Inspection	100% of incidents reported are addressed within 2 hours of initial notification and are resolved within 24 hours of initial notification.
Ensures the accuracy of contractor contact information and the site specific information	Measures the accuracy of contractor contact information and site specific information.	Periodic Inspection	100 % of records are complete and accurate
Measures the quality and timeliness of the patch management process	Executes the Patch Management Full Report for all systems at each assigned site	Periodic Inspection	100% compliance
Measures the risk level as reported through Tivoli	Executes the Patch Management Full Report for all systems at each assigned site	Periodic Inspection	100% compliance

Video Teleconferencing Support TASK 2: Customer Service Support			
Percentage of time the video-teleconferencing systems are available during the period.	Measures the availability of CBP managed video-teleconferencing systems.	100% inspection	Video-teleconferencing system availability $\geq 99.99\%$
Resource Management Support TASK 3			
Percentage of the accountability of assigned equipment to CBP managed sites	Measures the accountability of assigned equipment to CBP managed sites	100% inspection	100 % assigned items verified
Disposal of Excess Equipment TASK 3: Resource Management Support			
Measure the return time of equipment awaiting sanitization or preparation of excising,	Measures the amount of time it takes to complete the sanitizing or preparing excess equipment.	Periodic Inspection	$\leq 14$ days
TASK 4: Wide Area/Local Area Network Support			
Measures the availability of the network services to CBP managed sites.	Measures the percentage of response time each site is available during the period.	Periodic Inspection	CBP Site availability $\geq 99.99\%$
Measures the response time of the network services to CBP managed sites.	The average response time of a round trip Internet Control Message Protocol (ICMP) message between the CBP Network and Security Operations Center and the contractor's workstation.	Periodic Inspection	Average response time $\leq 250$ milliseconds
Measures the correct installation and configuration of a Cisco switch IAW CBP Standards.	Install and configure a Cisco switch	Periodic Sampling	Quality Assurance check must indicate no errors per switch.

Telecommunication Support TASK 6			
<p>Measures the performance and responsiveness to user calls that generate phone service tickets for adds, moves, or changes.</p>	<p>Measure time to respond to user requests via the CBP Help System (Remedy).</p>	<p>Periodic Inspection</p>	<p>Resolution of all service requests within 12 hours, defined by a count of the number of hours required to resolve the incident. Time runs continuously from ticket submittal.</p> <p>Upon completion of an issue, the ticket is marked as Resolved, the Remedy timer is stopped and a notice is sent to the customer. The customer shall be given the option of concurring that the issue is resolved or reopening the issue.</p> <p>The customer shall be given five business days to respond, after which time the ticket may be closed.</p> <p>If the customer does not concur, the ticket is reopened and the Remedy timer resumes. The ticket shall continue to be worked to resolve the customer concerns.</p> <p>Conflicts shall be resolved by the customer POC and the Operations &amp; Maintenance Branch Chief and/or Area Manager, as appropriate.</p>
<p>Measures the availability of the CBP managed phone systems.</p>	<p>Measure the percentage of time the telecommunications infrastructure is available during the period</p>	<p>Periodic Inspection</p>	<p>Telecommunication Infrastructure availability <math>\geq 99.99\%</math></p>

Measure the time it takes to restore phone system availability to the end user.	Measure the time to restore phone system connectivity.	100% of related tickets	The contractor shall restore normal phone system operations /connectivity $\leq$ 4 hours.
Measures the availability of the CBP managed phone systems.	Measure the percentage of time the file and print infrastructure is available during the period	Periodic Inspection	File and Print Infrastructure availability $\geq$ 99.99%
<b>TASK 7: FMITI</b>			
Measures the correct installation and configuration of a Novell/Microsoft File Server IAW CBP Standards.	Install and configure a Novell/Microsoft File Server	100 Percent Inspection	Quality Assurance check must indicate less than two errors per server.
Measure the time it takes to restore normal server operations and connectivity to the network.	Measure the time to restore network connectivity.	Random Sampling	The contractor shall restore normal file server operations /connectivity less then 4 hours.  If the server requires re-building the timeframe should not exceed 36 hrs.
<b>TASK 8: Project Management Support and Deployment</b>			
Measure the timely submission of circuit orders to facilitate move, construction or expansion of a CBP facility.	Gathering requirements and coordination of circuit order submission.	Periodic Inspection	100% of orders placed are correct and submitted within the required timeframe to facilitate the project requirement date.
Measure the timely submission of cabling requirements to facilitate move, construction or expansion of a CBP facility.	Gathering requirements and coordination of cabling order submission	Periodic Inspection	100% of orders placed are correct and submitted within the required timeframe to facilitate the project requirement date.
Measure the timely submission of equipment orders to facilitate move, construction or expansion of a CBP facility.	Gathering requirements and coordination of equipment order submission	Periodic Inspection	100% of orders placed are correct and submitted within the required timeframe to facilitate the project requirement date.
Measure the customer satisfaction of the	Determine the level of customer satisfaction	Random Sampling	The results shall indicate an average

contractor support	as it relates to facilities projects		customer feedback should be positive. Negative feedback shall be reported to the Deployment Manager.
Measure the attendance and contribution as a representative in meetings	Attend meetings and interpret the deployment responsibilities. Capture action items as well as future milestones	Random Intervals	Contractor shall capture, document, and notify management of action items

## 6.2 Network and Security Operations Center, DHS OneNet

### 6.2.1 Performance Metrics

The contractor shall assist in the development of the NSO performance and business metrics for each of the supported tasks relating to the NSO. These metrics will represent tangible and concise measures of success for the tasks defined in the SOW and will be used to track Contractor progress in meeting the NSO objectives.

### 6.2.2 Standard Operating Procedures (SOPs), Tactics Techniques Procedures (TTPs) and Operating Instructions (OIs)

The contractor shall develop and maintain formal, documented NSO SOPs, TTPs and OI's. The SOPs, TTPs, and OIs provide the operational basis for the DHS NSO Concept of Operations (ConOps), NSO Memorandums of Agreements and NSO Center to Center Guidelines, and any Memorandum of Agreement between DHS/CBP NSO and the Component NSO's. The Contractor shall submit the draft NSO SOP, TTP and/or OI for Government review within 20 days of contract award and these procedures will be reviewed and updated on an annual basis and/or as needed from the date of approval.

#### 6.2.2.1 Service Level Objectives

A service level objective (SLO) is a formal written agreement made between two parties; the service provider and the service recipient. It defines the expected level of services, the metrics associated with these services and the acceptable and unacceptable service levels. CBP/OneNet NSO SLOs are monitored via automated tools for Managed Services. As additional managed services and/or component services are subscribed too the contractor shall develop formal SLO's in a Memorandum of Agreement between the CBP/OneNet NSO to Component NSOs and or Managed Service Providers. In addition the contractor shall ensure metrics tracking and reporting of all SLOs utilizing automated monitoring tools.

### 6.3 Technology Service Desk

#### 6.3.1 Performance Measures

Measurement Area	Measurement Detail or Tracking Source	Target
Production Server Availability awareness	An updated Remedy problem ticket with Urgent Priority Notification Notifications; Symon Alert System, Remedy Bulletin Boards - Auto Operations/ SITROOM and TSD	>= 99.5% of all outages
Production Server Availability awareness	Notifications; by Warm Transfer & Remedy incident records - escalated to various queues or groups	>=99.5% of all outages
Technology Support Tier One Support Staff Answer Speed	Call Management System	Speed to answer <= 120 seconds
Technology Support Tier One Support Staff  Per support staff associate	First call resolution calculated as the number of inbound call records closed divided by the number of inbound calls answered. Number of tickets opened with proper POC and related information. Quick tickets closed with proper information, i.e. Update notes, update resolution in work tickets. Remedy will be used to determine First Call Resolution.	First call resolution >= 50%
Technology Tier One staff statistics:	Calls answered, out bound calls, staffed time, aux time, reason for aux time, RONA, ring no answer call, Staff is logged in and not on another call and chooses not to answer call or walks away from desk while available to receive phone call. CMS will be used to determine statistics.	33.5 hours availability to take calls per week per person; with a 6.5 hour in other AUX code, i.e., Meeting, Working in queue, training, break, lunch, etc.  .05% Ring no Answer, RONA calls per performance review
Technology Support Staff / Per associate best level of effort	CMS will be used to determine statistics.	Abandon rate <= 3%
Technology Support	Routing of incident Records to the	0%

Measurement Area	Measurement Detail or Tracking Source	Target
Staff / Per associate	correct group/Remedy queue with appropriate information.	
Technology Support Staff	Customer Complaints by customers on survey form and based on rating.	.05% of calls received.

Measure	Source	Formula	Process
Production Server Availability Awareness conducted through Auto Operations/ SITROOM and TSD	REMEDY, Big Fix, Manage Objects	An updated Remedy problem ticket with Urgent Priority Notification Automated Systems application, "Manage Objects".	>= 99.5% of all outages
First Call Resolution Incident Records	Remedy & CMS	Number of Call Records closed. Number Answered Calls	Query Remedy for all call and problem records with call method equal to "reported by telephone", email, & fax Answered phone calls per Remedy
Calls answered, out bound calls, staffed time, aux time, reason for aux time, RONA, ring no answer calls,	Call Management System Application	CMS – Staffing Average & daily numbers of all Speed to Answer times	CMS, Each associate and Group
Abandon Rate	Call Management System Application	Abandoned Calls  Total Calls (excludes calls abandoned in less than 15 seconds)	CMS Supervisor, Select historical data, Each associate and Group Select report Skill Daily, Use "% Abandoned" field for value
Surveys and customer complaints	Remedy/Customer	Complaints by customers	Documented customer complaints
Surveys	Customer Satisfaction Survey	Complaints by customers on survey form and based on rating.	Customer satisfaction surveys sent to 100 random customers, (contractor and

Measure	Source	Formula	Process
			government employees) that were serviced by the Technology Service Desk during the performance review option period.

#### 6.4 Program and Project Management

None applicable.

#### 7 CONTRACT TYPE

This acquisition is a time and material contract.

#### 8 DELIVERABLES AND DELIVERY SCHEDULE

All deliverables produced as a result of this Statement of Work shall become the property of the Government. The Contractor shall deliver two (2) hard copies and one (1) softcopy (electronic media using Microsoft applications) to the COTR at the address specified in this Statement of Work unless otherwise specified.

All reports, plans, and other materials shall be provided in a Contractor-provided format; however, all deliverables must be supplied using Microsoft Office products.

##### 8.1 Information Technology Field Services Support

Number	Title	SOW Paragraph Reference Number	Final Due Date
1	<b>Kick Off Meeting with Contractor</b> Provide Briefing Slides on Staffing & Transition, Clearance, Hiring – Program Managers and Key Personnel to Attend.	3.4.1	5 business days after award
2	<b>Staffing Reports</b> with an overview of current staffing and recruiting efforts. These reports shall be deemed accepted upon delivery. This report can be changed at the discretion of the COTR and shall be defined upon the outset of this award.	3.4.1, 9	Initial draft with Contractor’s Proposal; Final submission 10 calendar days after completion of Kick-Off Meeting and then Weekly thereafter

3	<b>Remedy Ticket Management Reports</b>	5.1.1.1.2	Daily (Open and Closed Call)
4	<b>Differential and Full backups of all production servers for the specified sites</b>	5.1.1.1.2	Daily and weekly
5	<b>Ad Hoc Reports, such as, Trip reports;</b> <ul style="list-style-type: none"> <li>• Meeting agenda reports;</li> <li>• Meeting minutes;</li> <li>• Other reports required by the COTR.</li> </ul>	5.1.1.11	As Required; agenda submissions five (5) days before meetings; Minutes are due five (5) days after meetings.
6	<b>Integrated Baseline Reviews</b>	5.1.1.8	First IBR shall be conducted within 90 calendar days after award; Initial draft of Agenda and review materials to COTR 10 business days before scheduled event If initial draft is approved, this will constitute final submission; If initial draft is not approved, Contractor has 5 calendar days to submit in final
7	<b>Security Documentation – Contractor Information Technology (IT) Security Plan and IT Security Accreditation</b>	App B	Initial draft of Plan due 15 business days before final submission Final Plan due within 60 calendar days after award of contract Written proof of IT Security Accreditation due 6 months after award of contract
8	<b>Cost Performance Reports (Format 1) and Variance Reports (Format 5)</b>	App B	Before contract award and with response to the Solicitation, the Contractor shall submit a tailored or alternate report format. However, in all cases, the alternative must conform to EVMIG and ANSI/EIA – 748 A Standards.  Due by the 15th calendar day of a month; Accompanies the Monthly Status Reports Updates to these reports are required if the COTR requires further information, which he/she shall submit, in writing, no later than ten (10) business days following receipt of report.
9	<b>Contractor Employee List of Completed background Investigations and Procedures for Input and Tracking</b>	App B	List of Employees required 10 business days after award; Immediate notification to COTR of completed Background Investigations; Input into CBP Centralized Contractor Tracking System before receiving facility access badges
10	<b>Contractor Employee Separation Procedures</b>	App B	Submission of CF-242 Form for all departing Contractor personnel; Notification in writing of separating Non-Key personnel one day prior to separation;

			Written notification of substitution of Key Personnel 15 business days before expected initiation; or 30 business days prior if a Background Investigation is required
<b>11</b>	<b>Project Accounting Report</b>	App B	Monthly
<b>12</b>	<b>Project Tracking System</b>	5.1.1.8.1	Submission 60 calendar days after award; updates are required within five (5) business days of notification of changes

## **8.2 Network and Security Operations Center, DHS OneNet**

### **8.2.1 Reporting Requirements**

#### **8.2.1.1 Daily Situational Awareness Brief**

The Contractor shall facilitate a daily NSO Enterprise Situational Awareness Brief with the DHS/CBP leadership. This brief will be in micro-soft power point and will include all Network Operations events. The government will provide the contractor with the format of the Daily Situational Awareness Brief within 10 days of contractor award. In addition the Contractor shall recommend and develop way ahead to automate the situational awareness brief to the leadership and enterprise components.

#### **8.2.1.2 Daily Status Report**

The Contractor shall facilitate a daily NSO operational conference call with the duty officer, and provide daily status report to support the DHS/CBP NSO operations. The Contractor shall submit NSO input to the agenda and updated detailed activity will be provided daily by 0600 A.M. Conference call information includes any reported Component Network outage, Network event notifications, Network device outages, alerts, Firewall issues, major network configuration changes and bandwidth anomaly in the previous 24 hours. This information may be accessed by authorized users to retrieve ad-hoc reports using the CBP/DHS NSO On-Line web portal, The Contractor shall maintain the website, administer users and update continuously to provide real-time information for the daily conference call NSO report.

- Network infrastructure outage reports
- Network firewall outages/anomaly reports
- Bandwidth anomaly issues
- Network device outages/anomalies
- Top 100 circuit outages/anomalies
- Significant component network issues/anomalies

#### **8.2.1.3 Weekly Status Reports (Bandwidth, Ticketing, Budget, Personnel)**

The written weekly report shall consist of a summary of all NSO activities and reference analysis of NSO performance metrics, track status of network events, by category, tickets, call logs,

investigatory cases, network event notifications, issues & risks and actions accomplished for the week. This report shall be prepared by the NSO Project Manger and shall be presented to the OTM by noon Wednesday for inclusion into the Technical Operations Division (TOD) weekly report CBP Office of Information Technology.

#### **8.2.1.4 Monthly Program review Reports (Bandwidth, Ticketing, Budget, Personnel)**

The Contractor shall submit monthly status reports to the OTM, the Contracting Officer Technical Representative (COTR) and the Contracting Officer (CO) on the progress made during the respective reporting period in performance of the work requirement. The report shall address work completed during the current period, planned activities, and problems/issues with recommended solutions, anticipated delays, and resources expended. If applicable, any trip reports and significant results. The report shall include planned work assignments and desired results for the next reporting period. The reports shall be detailed to provide an ongoing record of all support efforts. For each task area, the Contractor shall provide a budget including cumulative expenditures and balance remaining, hours utilized by employee name and labor category for the month and cumulative hours utilized by employee name and labor category for the period of performance for the contract.

This report shall be submitted within 5 calendar days following the end of each work month. Each work month is defined as 30 consecutive calendar days. The report shall be delivered in one hard copy and one electronically provided (email) soft copy in a format to be agreed upon with the OTM.

#### **8.2.2 Briefing/Meetings**

Each briefing/meeting shall cover the essential elements of the relevant subject matter and an agenda and meeting minutes shall be prepared and presented in a clear, concise and orderly manner. Appropriate briefing tools such as Microsoft Power Point, overhead slides, plotted charts, etc., shall be used. Hardcopy handouts of all briefing materials shall be made available to all attendees prior to, or at the time of the briefing.

#### **8.2.3 Periodic Meetings**

CBP OTM will coordinate periodic meetings and reviews to ensure all relevant provisions of the task order are being met. The Contractor shall meet with the COTR to discuss their performance monthly at a minimum.

#### **8.2.4 Deliverables Table**

The work products shall be delivered in accordance with the schedule set forth in the table above. The Contractor shall refer to Section 4 for place of and method of delivery to CBP.

##### **8.2.4.1 Deliverable Requirements Delivery Schedule**

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
1	Project Management	5.22	Within	COTR will be	OTMs, COTR,

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
	Plan		20 days after contract award	given 5 business days to review and comment, with Final due 5 business days after COTR comment	Contract Project Manager
2	Performance Metrics	8.2.1.3	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager
3	Presentations	5.2.2	Provide documents per the direction of the OTM	As Required	Applicable OTMs and Programs Managers
4	Standard Operating Procedures; Tactics Techniques & Procedures and/or Operating Instructions	6.2.2	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, applicable OTM
5	Service Level Objectives	6.2.2.1	As required	As required	OTMs, COTR, Contract Project Manager, authorized DHS recipients, TPOCs
6	Briefings/Meetings	8.2.2	Attend and Provide documents per the direction of the OTM	As Required	Applicable OTMs and Programs Managers
7	Periodic Meetings	8.2.3	Attend and Provide documents per	As Required	Applicable OTMs and Programs Managers

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
			the direction of the OTM		
8	Engineering Change Request (CR) review	Will provide document upon award	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, TPOCs
9	Maintain NSO Certification & Accreditation (C&A) Documentation	Will provide document upon award	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, authorized DHS recipients, TPOCs

**8.2.4.2 Reporting Requirements Delivery Schedule**

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
10	Activity Service Level Offering Compliance Report	6.2.2.1	Weekly	Weekly	OTMs, COTR, Contract Project Manager, applicable DHS recipients OTM
11	Daily Situational Awareness Brief	8.2.1.1	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR Contractor PM
12	Daily Status Report	8.2.1.2	Within 30 days after contract award	Daily	OTMs, COTR, Contract Project Manager, applicable DHS recipients OTM
13	Weekly Status Reports	8.2.1.3	Within 30 days after contract award	Weekly	OTMs, COTR, Contract Project Manager, applicable DHS recipients OTM
14	Monthly Program review Reports	8.2.1.4	Within 30 days	Monthly	OTMs, COTR, Contract Project

			after contract award		Manager, applicable DHS recipients OTM
15	Monthly Cost Reports	9.4	Monthly	Monthly	OTM, COTR
16	Monthly Status Monitoring and Analysis Reports	8.2.1	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR Contractor PM

### 8.3 Program and Project Management

#### 8.3.1 Project SELC Artifacts

The Contractor shall ensure delivery of all project and SELC related documentation and artifacts consistent with scope of this task. If CBP utilizes an equivalent document, the CBP document template shall be utilized. The delivery schedule for project related documentation/artifacts tasked to the Contractor shall be dictated by the respective project schedule, developed by the Contractor, and shall be considered late if the final version of the document is not submitted in accordance with the respective project schedule.

#### 8.3.2 Project Cost Management Artifacts

Project cost and project EVM information and reports shall be developed, maintained and reported at defined times throughout the duration of this task. Project EVM information shall be accurate to within one week and reports shall be readily available upon ad hoc request.

#### 8.3.3 Project Schedule Management Artifacts

Individual project Work Breakdown Structures (WBS) and related project schedules shall be developed, baselined, maintained and monitored as per project management and SELC principals.

#### 8.3.4 Integrated Master ITP Program Schedule

The Contractor shall coordinate, develop, baseline, maintain and monitor an Integrated Master Program Schedule, to meet objectives as defined within this SOO.

#### 8.3.5 Briefings, White Papers, Presentations

The Contractor shall prepare program/project specific technical briefings, white papers and presentations, as requested. These presentations will typically be prepared in Microsoft PowerPoint and Visio.

#### 8.3.6 Program/Project Meetings

The Contractor shall attend each briefing/meeting that is specific to the relevant program/project technical subject matter. The Contractor shall prepare an agenda and meeting minutes and present the agenda and minutes in a clear, concise and orderly manner. Appropriate briefing tools such as Microsoft PowerPoint, overhead slides, plotted charts, etc., shall be utilized. Hardcopy

handouts of all briefing/meeting materials shall be made available to all attendees prior to, or at the time of the briefing. Meeting minutes shall be developed and distributed to meeting invitees and updated as required.

### **8.3.7 Standard Operating Procedures (SOPs), Tactics Techniques Procedures (TTPs) and Operating Instructions (OIs)**

The Contractor shall recommend, develop, and maintain formal, documented ITP specific SOPs, TTPs and OI's. The SOPs, TTPs, and OIs provide the operational basis for the ITP operations. The Contractor shall submit the draft SOP, TTP and/or OI for Government review and these procedures will be reviewed and updated on an annual basis, at minimum, or as needed as directed by the COTR.

### **8.3.8 Reporting Requirements**

#### **8.3.8.1 OneNet Circuit Order Status Report**

The Contractor shall maintain a tracking system for OneNet circuit order status containing identification and details of each circuit order request, including circuit specifications, site address details, requested delivery date, vendor anticipated delivery date, delivery status, risks, issues and other circuit order related information of value. Other circuit status reporting information may be requested by the Government. Upon request by the COTR, the Contractor shall generate an ad hoc status report reflecting current status of either individual or an aggregate of circuit orders.

#### **8.3.8.2 Weekly Project Status Reports**

The written weekly report shall consist of a summary of accomplishment for each project; milestones achieved or missed, performance metrics, status of implementation activities, issues and risks with applicable impact and mitigation, and planned accomplishments for the proceeding week. Two reports shall be prepared one in quad chart format the other in paragraph format. These reports shall be prepared and shall be presented to the COTR or Task Monitor by noon Wednesday for inclusion into the ITP weekly report for OIT.

#### **8.3.8.3 Project Program Management Reviews**

The CBP CIO, on a quarterly basis, conducts Program Management Reviews (PMR) of each project. PMR data is stored in CBP's WorkLenz application. In addition to project performance, Government Project Managers must report on earned value management, scope, schedule, cost, risks/issues, and enterprise architecture at the PMR. The Contractor shall be responsible for maintaining project information within WorkLenz throughout the project lifecycle.

#### **8.3.8.4 Periodic Contract Meetings**

The Contractor shall meet monthly, or as requested, with the COTR and Task Monitor to discuss task performance.

#### **8.3.8.5 Task Order Status Reports**

The Contractor may be required to submit monthly status reports to the Task Monitor, the COTR and the Contracting Officer (CO) on the progress made during the respective reporting period in performance of the work requirement. The report shall address work completed during the current period, planned activities, and problems/issues with recommended solutions, anticipated delays, and resources expended. If applicable, any trip reports and significant results. The report shall include planned work assignments and desired results for the next reporting period. The reports shall be detailed to provide an ongoing record of all support efforts. For each task area, the Contractor shall provide a budget including cumulative expenditures and balance remaining, hours utilized by employee name and labor category for the month and cumulative hours utilized by employee name and labor category for the period of performance for the contract.

This report shall be submitted within 5 calendar days following the end of each work month. Each work month is defined as 30 consecutive calendar days. The report shall be delivered in one hard copy and one electronically provided (email) soft copy in a format to be agreed upon with the OTM.

#### **8.3.9 Program Management and Administrative Services**

The Contractor shall provide general administrative support and other direct charge support. Professional services to be performed will include but are not limited to the following:

- The Contractor shall provide on-site clerical and administrative support to the ENTS. Tasking will include generating and maintaining of program and project files and database, and preparing and distributing of project reports and supporting documentation.
- The Contractor shall also provide facilities and supplies for hosting meeting and conferences; preparing overhead transparencies and slides; printing and copying services; communication services (voice, video, and data) and overnight mail services.
- The Contractor shall provide professional support to assist in program management functions, it includes, but not limited to, financial analysis, cost benefit and earned value support, logistics support, training support, and schedule support.

#### **8.3.10 Quality Control**

The Contractor shall establish and maintain a complete Quality Control Plan (QCP) to ensure that the objectives of this task order are provided as specified. The QCP shall describe the methods for detecting, identifying and preventing problems before the level of performance becomes unacceptable. One copy of the Contractor's QCP shall be provided to the Contracting Officer (CO) at the time their contract is submitted. A detailed QCP should be submitted sixty days from award of the contract. An updated copy of the QCP must be provided to the CO as changes occur.

### **8.3.11 Project SELC Artifacts**

The Contractor shall ensure delivery of all project and SELC related documentation and artifacts consistent with scope of this task. If CBP utilizes an equivalent document, the CBP document template shall be utilized. The delivery schedule for project related documentation/artifacts tasked to the Contractor shall be dictated by the respective project schedule, developed by the Contractor, and shall be considered late if the final version of the document is not submitted in accordance with the respective project schedule.

### **8.3.12 Project Cost Management Artifacts**

Project cost and project EVM information and reports shall be developed, maintained and reported at defined times throughout the duration of this task. Project EVM information shall be accurate to within one week and reports shall be readily available upon ad hoc request.

### **8.3.13 Project Schedule Management Artifacts**

Individual project Work Breakdown Structures (WBS) and related project schedules shall be developed, baselined, maintained and monitored as per project management and SELC principals.

### **8.3.14 Integrated Master ITP Program Schedule**

The Contractor shall coordinate, develop, baseline, maintain and monitor an Integrated Master Program Schedule, to meet objectives as defined within this SOW.

### **8.3.15 Briefings, White Papers, Presentations**

The Contractor shall prepare program/project specific technical briefings, white papers and presentations, as requested. These presentations will typically be prepared in Microsoft PowerPoint and Visio.

### **8.3.16 Program/Project Meetings**

The Contractor shall attend each briefing/meeting that is specific to the relevant program/project technical subject matter. The Contractor shall prepare an agenda and meeting minutes and present the agenda and minutes in a clear, concise and orderly manner. Appropriate briefing tools such as Microsoft PowerPoint, overhead slides, plotted charts, etc., shall be utilized. Hardcopy handouts of all briefing/meeting materials shall be made available to all attendees prior to, or at the time of the briefing. Meeting minutes shall be developed and distributed to meeting invitees and updated as required.

### **8.3.17 Standard Operating Procedures (SOPs), Tactics Techniques Procedures (TTPs) and Operating Instructions (OIs)**

The Contractor shall recommend, develop, and maintain formal, documented ITP specific SOPs, TTPs and OI's. The SOPs, TTPs, and OIs provide the operational basis for the ITP operations. The Contractor shall submit the draft SOP, TTP and/or OI for Government review and these procedures will be reviewed and updated on an annual basis, at minimum, or as needed as directed by the COTR.

### **8.3.18 OneNet Circuit Order Status Report**

The Contractor shall maintain a tracking system for OneNet circuit order status containing identification and details of each circuit order request, including circuit specifications, site address details, requested delivery date, vendor anticipated delivery date, delivery status, risks, issues and other circuit order related information of value. Other circuit status reporting information may be requested by the Government. Upon request by the COTR, the Contractor shall generate an ad hoc status report reflecting current status of either individual or an aggregate of circuit orders.

### **8.3.19 Weekly Project Status Reports**

The written weekly report shall consist of a summary of accomplishment for each project; milestones achieved or missed, performance metrics, status of implementation activities, issues and risks with applicable impact and mitigation, and planned accomplishments for the proceeding week. Two reports shall be prepared one in quad chart format the other in paragraph format. These reports shall be prepared and shall be presented to the COTR or Task Monitor by noon Wednesday for inclusion into the ITP weekly report for OIT.

### **8.3.20 Project Program Management Reviews**

The CBP CIO, on a quarterly basis, conducts Program Management Reviews (PMR) of each project. PMR data is stored in CBP's WorkLenz application. In addition to project performance, Government Project Managers must report on earned value management, scope, schedule, cost, risks/issues, and enterprise architecture at the PMR. The Contractor shall be responsible for maintaining project information within WorkLenz throughout the project lifecycle.

### **8.3.21 Periodic Contract Meetings**

The Contractor shall meet monthly, or as requested, with the COTR and Task Monitor to discuss task performance.

### **8.3.22 Task Order Status Reports**

The Contractor may be required to submit monthly status reports to the Task Monitor, the COTR and the Contracting Officer (CO) on the progress made during the respective reporting period in performance of the work requirement. The report shall address work completed during the current period, planned activities, and problems/issues with recommended solutions, anticipated delays, and resources expended. If applicable, any trip reports and significant results. The report shall include planned work assignments and desired results for the next reporting period. The reports shall be detailed to provide an ongoing record of all support efforts. For each task area, the Contractor shall provide a budget including cumulative expenditures and balance remaining, hours utilized by employee name and labor category for the month and cumulative hours utilized by employee name and labor category for the period of performance for the contract.

This report shall be submitted within 5 calendar days following the end of each work month. Each work month is defined as 30 consecutive calendar days. The report shall be delivered in

one hard copy and one electronically provided (email) soft copy in a format to be agreed upon with the OTM.

**8.3.23 Deliverables Tables**

The work products and reports shall be delivered in accordance with due dates listed in the following tables:

**8.3.24 Deliverable Requirements Delivery Schedule – Technical Point of Contact(s) (TPOC) will be designated at the kick-off of each project**

No	Title/Soft Copy Format	SOW Section/P aragraph	Draft Due	Final Due Date	Recipient(s)
1	Project management artifacts and SELC documentation	3.4.1 8.4.11	As defined by respective project schedule	Various but shall not impact project milestones and ultimate project success	ITP Gov't Project Manager, Technical Points of contact (TPOC), COTR/Task Monitor (s)
2	Project Cost Management Artifacts, i.e., project cost estimates, project cost performance, EVM documents, WBS	3.4.1 9.4 8.4.12	As defined by respective project schedule	Various per schedule, Cost performance and EVM shall be available upon request	ITP Director, ITP Gov't Project Manager, Technical Points of contact, COTR/Task Monitor (s)
3	Project Schedule Management Artifacts, i.e., WBS, project schedule	8.4.13	As defined by SELC and respective period for which these artifacts are to be developed upon project initiation	Various so as not to impact project success	ITP Gov't Project Manager, Technical Points of contact, COTR/Task Monitor (s)
4	Integrated Master Schedule	8.4.14	45 days following contract award	Approved format 60 days following contract award,	COTR/Task Monitor (s), ITP Director ITP Gov't Project

No	Title/Soft Copy Format	SOW Section/Paragraph	Draft Due	Final Due Date	Recipient(s)
				following that it recognized the schedule will be a living document	Managers
5	Briefings, White Papers and Presentation documents	8.4.15	As required	Various	ITP Gov't Project Managers, ITP Director, ITP Staff, TPOCs, COTR/Task Monitor (s)
6	Meeting Artifacts	8.4.16	As required	Various	ITP Gov't Project Managers, ITP Director, meeting invitees, COTR/Task Monitor (s)
8	Standard Operating Procedures; Tactics Techniques & Procedures and/or Operating Instructions	8.4.17	Within 45 days after contract award	Within 60 days after contract award. Reviewed annually and revised as needed.	Task Monitor, COTR/Task Monitor (s) ITP Gov't Staff

**8.3.25 8.11.2 Reporting Requirements Delivery Schedule**

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
10	OneNet circuit status reports	8.4.18	Within 20 days from award	Within 30 days from award	ITP OneNet Task Monitor, TPOCs, COTR/Task Monitor (s)
11	Weekly Project Status Reports	8.4.19	Within 10 days after contract award	Weekly	Task Monitor, ITP Director, applicable DHS recipients, COTR/Task Monitor (s)
12	Program Management Review	8.4.20	Within 10 days after contract award	Bi -monthly	ITP Director, ITP Gov't Leads, TPOCs, various DHS

					representatives, COTR/Task Monitor (s)
13	Periodic Meetings	8.4.21	As required	As required	COTR, Task Monitor(s)
14	Task Order Status Reports	8.4.22	Within 30 days after contract award	Monthly or as required	COTR, Task Monitor(s), Contracting Officer

#### 8.4 Acceptance Requirements of Deliverables

General quality measures, as set forth below shall be applied to each work product received from the Contractor. The expected quality of Contractor produced work products shall adhere to existing federal, DHS and CBP policy and standards.

**Accuracy** – Work products shall be accurate in technical and grammatical content and shall be based upon the intended scope of the applicable program/project.

**Clarity** – Work products shall be clear and concise; engineering or technical terms shall be used as appropriate to the intended audience. All diagrams shall be easy to understand and be relevant to the supporting narrative.

**Conformance to Requirements** – All work products shall satisfy the requirements of the work request. The project work products shall adhere to CBP System Lifecycle (SELC) and DHS based templates, standards and directives.

**File Editing** – All text and diagrams, developed as Government owned products, and shall be provided in a format that is editable by the Government, unless specified.

**Format** – Work products shall be submitted in Microsoft Office and currently approved CBP application version. Hard copy formats shall follow CBP/DHS Directives and shall be consistent with similar efforts.

**Timeliness** – Work products shall be submitted on or before the due date specified in the Work Request or submitted in accordance with a later scheduled date determined by the Government.

### 9 INVOICE REQUIREMENTS/PERIOD OF INVOICE

Invoices shall be submitted for all costs accrued during the monthly reporting period using the following guidelines:

- The monthly reporting period may be a calendar month or any other period used by Contractor as a billing cycle, provided that this billing cycle has no fewer than 28 and no more than 31 days in it.
- Invoices shall separately identify costs for each task order or modification.

- Invoices shall only include charges for that specific billing period. If a charge is not within the billing period listed on the invoice, a new invoice shall be submitted.
- Original invoices are submitted to:
  - DHS – Customs and Border Protection
  - PO Box 68908
  - Indianapolis, IN 46268
- Copies of the invoices shall be submitted to the COTR in hard copy and electronically by email and to [CBPinvoices@dhs.gov](mailto:CBPinvoices@dhs.gov).
  
- Invoices shall be submitted within ten (10) working days of the end of the Contractor's billing cycle.
- Invoices shall contain the following information:
  - Company name and address
  - Name and address of person to whom payment is to sent, including EFT information, if applicable.
  - Name, title, and phone number of person to notify in the event of defective invoices.
  - The period being invoiced. This must include the beginning and end dates (dd/mm/yyyy format) of the calendar month or billing cycle period being invoiced.
  - Task Order Number (or Task Order Modification Number).
  - Total Value of Task Order (or Task Order Modification Value).
  - Task Order Period of Performance.
  - Monthly hours by labor category, and, broken out within each labor category, monthly hours by individual employee.
  - Labor Category Rates.
  - Total cost by task or CLIN, labor category and by individual employee.
  - Summary Tabulation (cumulative) as follows:
    - Summary hours, to date, by labor category.
    - Labor Category Rate.
    - Total cost, to date, by task or CLIN, and by labor category.
- Certification by a competent company official that the invoice contains all accrued costs for the month to the best of the official's knowledge.
- The following information is required to report Travel costs accruals (per individual trip):
  - Date (start and end) for travel
  - Task or CLIN Number
  - Travel description
  - Travel breakdown (per diem, airfare, care rental, mileage, etc.)
  - Copy of COTR documentation approving the travel
  - Total price for travel, by trip and total for all travel

## 9.1 Travel

Travel to any of the Component locations may be required. Travel will be performed in accordance with the Federal Travel Regulations (FTR). The COTR/Task Monitor shall identify travel requirements on a case by case basis. The COTR/Task Monitor must approve all travel requests. Any travel shall be in accordance with the Federal Travel Regulations (for travel in 48

contiguous states), the Joint Travel Regulations, DoD Civilian Personnel, Volume 2 Appendix A (for travel to Alaska, Hawaii, Puerto Rico, and U.S. territories and possessions), and if required by the SOW, the Standardized Regulations (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" (for travel not covered in the Federal Travel Regulations or Joint Travel Regulations).

Contractor personnel working at a government site for any length of time will not be paid local travel costs when traveling to or from the work site. Other local travel costs shall be allowed if requested in advance by the Contractor and with written consent from the COTR/Task Monitor.

## **9.2 Other Direct Costs.**

Travel and ODCs will be estimated and burdened with the ODC markup percentage specified in the contract. Profit on travel and ODCs is not allowable. The cumulative extended total of all labor categories ordered plus travel and ODCs will define the overall ceiling price. The Contracting Officer may authorize adjustments between labor category quantities of up to 10%, within the established task labor ceiling price, without a formal modification. Labor dollars will not be used to pay for ODCs nor ODC dollars used to pay for labor without a contract modification.

At any time and throughout the life of the contract, at the request of either the Contractor or the Government, the Contractor may modify the mark-up percentages for Other Direct Costs (ODCs) based on the Contractor's audited ODC percentage rate for its fiscal year. These modified ODC percentages will be negotiated on a case-by-case basis. The modified ODC percentage rate, upon determination by the Government that they are based on DCAA or other Government audit information, will be incorporated by modification.

## **9.3 Project Accounting Reports**

The Contractor shall provide monthly reports, by project, that provide, at a minimum, the following information:

- Employee's Name
- Work Location
- Name(s) of Project
- Regular and Overtime hours worked for each project worked
- Any associated reimbursable travel costs for each project worked

The Government will provide an initial list of project names that will require tracking at the Kick-Off Meeting. The COTR shall provide periodic updates to the initial project list as required. The Contractor shall implement a project tracking system within 60 calendar days after award of this contract. If updates are required, the Contractor shall implement any new project tracking within 5 business days after the project updates have been officially received by the Contractor.

## **9.4 Earned Value Management and Reporting**

In accordance with OMB Circular A-11, the Government will use Earned Value Management (EVM) to monitor tasks under this PWS. The Contractor shall provide EVM that meets the

criteria as defined in the current American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) Standard 748-2002, Earned Value Management Systems, approved May 19, 1998.

CBP requires that contracts and task orders in support of programs that have assets in the development, modernization, or enhancement phase will require the use of EVM to measure the cost, schedule, and performance of those assets against the established baseline. For contracts and task orders that are greater than or equal to \$5M, the Government requires full compliance with the ANSI/EIA Standard 748 (2002) guidelines, with self-verification. For those contracts and task orders that are less than \$5M but greater than or equal to \$1M, the Government requires compliance to a specific subset of the ANSI-748 guidelines, with self-verification. For contracts and task orders that are under \$1M annual cost, Earned Value Management is at the discretion of the COTR. The Contractor shall self-verify the compliance of its system. The Government reserves the right to apply the higher alternative EVMS standard to Prime Contractors that may have multiple task orders with a total cumulative value greater than \$5M and greater than \$1M. The Government reserves the right to obtain independent verification of a Prime Contractor's EVM system.

EVM Reports shall be submitted on a monthly basis after award.

In the performance of this Statement of Work, the Contractor shall use an earned value management system (EVMS) that complies with the criteria provided in ANSI/EIA-748, appropriately tailored (i.e., meets at least ten of the Intent Guidelines) to the task order and has been self verified.

If at any time during performance of the effort, the self verification is determined to be defective, the Contractor shall correct the defect at no additional cost to the government.

The Contractor shall provide the Contract Cost, Schedule, Forecast, and Performance Reports – Formats 1 and 5 in accordance with the requirements of this overall effort.

The Contractor shall participate in integrated baseline reviews; the first of which will be considered a Kick-Off Meeting and shall be scheduled five (5) days after award. Other such reviews shall be scheduled as early as practicable and should be conducted within 90 days after (1) contract award, (2) exercise of significant contract options, and (3) the incorporation of major modifications. The objective of the integrated baseline review is for the Government and the Contractor to jointly assess areas such as the Contractor's planning, to ensure complete coverage of the Statement of Work, logical scheduling of the work activities, adequate resourcing, and identification of inherent risks.

The Contractor shall provide an Integrated Master Schedule as part of each EVMS report.

The approved EVMS shall only be modified by written bilateral modification to the contract or task order.

The Contractor agrees to provide access to all pertinent records and data requested by the COTR or Contracting Officer to validate and verify the accuracy and completeness of the EVMS data

and ensure that the EVMS complies, and continues to comply, with the ANSI/EIA-748 standard referenced in paragraph (a) of this clause.

## **10 GOVERNMENT-FURNISHED PROPERTY, EQUIPMENT AND INFORMATION**

### **10.1 PROPERTY**

CBP intends that all support performed under this Statement of Work shall be accomplished by utilizing Government Furnished Property. Depending on availability of equipment and space at each site, CBP shall provide desk, a personal computer and/or laptop for access to CBP network. Contractor employees shall be made responsible for CBP issued Government Property personally assigned to him or her for personal use as deemed necessary to accomplish the tasking. All Government Furnished Property and Equipment shall be returned to the Government prior to separation of employee.

### **10.2 EQUIPMENT**

#### **10.2.1 Information Technology Field Services Support**

##### **10.2.1.1 Government Furnished Tools**

CBP shall provide to the Contractor access to an assortment of diagnostic tools. The diagnostic tools may include the following: ConsoleOne, iManager, Novell Remote Manager, Active Directory Users and Computers, RconsoleJ, ERD Commander, Power Quest/Norton Ghost (disk imaging software), Remedy and Dimensions.

#### **10.2.2 Network and Security Operations Center, DHS OneNet**

The Government will provide personnel with work areas equipped with a workstation, and have access to a printer, telephones, and general office supplies. Some work may be performed off-site. Any off-site work shall be coordinated and approved with the COTR.

##### **10.2.2.1 Government Furnished Tools.**

CiscoWorks, Concord eHealth/LiveHealth, Netcool, NetView, Tivoli, Solar Winds and other distributed processing-oriented management tools

#### **10.2.3 Technology Service Desk**

The Government will provide personnel with work areas equipped with a workstation, and have access to a printer, telephones, and general office supplies. Some work may be performed off-site. Any off-site work shall be coordinated and approved with the COTR.

#### **10.2.4 Program and Project Management**

The Government will provide on site Contractor personnel with work areas equipped with a workstation, and have access to a printer, telephones, and general office supplies as available. Some work may be performed off-site.

## **10.3 INFORMATION**

#### Government Furnished Information and Contractor Non-Disclosures

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this task and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the task. The Contractor will be requested to sign Non-Disclosure statements.

#### Protection of Government Information and Data

All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. Contractor shall conform to all security policies contained in the U.S. Customs and Border Protection Security Policies and Procedures Handbook, CIS HB 1400-05B.

All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, Information Technology Systems Security Program and 4300A Sensitive Systems Handbook."

All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, Information Technology Systems Security Program and 4300A Sensitive Systems Handbook."

### **10.3.1 Information Technology Field Services Support**

CBP shall make available to the Contractor all necessary related documentation, hardware, and software required to effectively provide support and services. This includes the items which are cited in Section 1.4 of this document; however, they may not be released to the general public per CBP security regulations. These documents include: Information Systems Security Policies and Procedures Handbook (1400.05c); CBP OIT "LAN Standards"; CBP OIT Outage Escalation Procedures; CBP OIT Disaster Recovery Procedures.

### **10.3.2 Network and Security Operations Center, DHS OneNet**

- System Life Cycle documentation;
- Separation Procedures for Contractor Employees;
- Information Systems Security Policies and Procedures documentation to be furnished upon award;
- Process Asset documentation;
- Technical Reference documentation;
- Current CBP LAN and OneNet enterprise architecture documentation;
- CBP LAN and OneNet Network, Directory, Messaging, Collaboration, and Engineering Documentation.

#### **10.3.2.1 Storage and Management of Government Finished Information**

- Contractor shall comply with storage and management of government finished information in accordance with direction from the OTM.

### **10.3.3 Technology Service Desk**

None applicable.

### **10.3.4 Program and Project Management**

The Government will establish a document library for vendors proposing so they may review contract related documents that are not readily available to the general public.

- System Engineering Life Cycle documentation
- Separation Procedures for Contractor Employees;
- Information Systems Security Policies and Procedures documentation to be furnished upon award;
- Process Asset documentation;
- Technical Reference documentation;
- CBP Security Guidelines

## **10.4 Property**

### **10.4.1 Government Owned Vehicles**

The Contractor shall have access, if available, to Government Owned Vehicles (GOV) for the sole purpose of official Government-approved temporary duty (TDY) or local travel. The use of a GOV shall be in accordance with all existing, applicable Federal Government regulations. The Contractor shall ensure that all its employees possess and maintain motor vehicle liability insurance covering bodily injury and property damage, in the amounts of \$200,000 per person and \$500,000 per occurrence for bodily injury and \$20,000 per occurrence for property damage, protecting the Contractor and the Government against third-party claims arising from the ownership, maintenance, or use of an Interagency Fleet Management System (IFMS) vehicle. The contractor shall possess proof of insurance and produce such upon request by the government. The Contractor shall assume, without the right of reimbursement from the Government, the cost or expense of any use of IFMS vehicles and services not related to the performance of the contract.

## **11 PLACE OF PERFORMANCE**

IT support Contractors shall be located at offices, as designated by CBP, located throughout the United States, Puerto Rico, Canada, Guam, and the Virgin Islands.

Due to the high volume of CBP and OIT Headquarters personnel located in the Washington D.C. and Northern Virginia metropolitan area, there shall be a larger percentage of Contractor employees located in this particular area. Primary locations include: Springfield, VA and Herndon, VA.

Supported locations shall not be limited to the Contractor's home duty office/location. In other words, the Contractor shall also provide support to CBP locations within their assigned regions.

At the discretion of the Government, remote access may be directed. This access will only use Government supplied connection devices. For support requiring on-site support, Contractor employees shall travel to the location. The extent of travel shall range from travel within the local metropolitan commuting area to as much as travel within an entire state, or nearby state(s).

As situations warrant, such as natural disasters, emergencies, deployment projects, Contractor employees shall be asked to travel to locations outside of their CBP Field Support regions, depending upon availability for periods up to three weeks.

Secondary, or alternate, site support, as well as rotational support, may also be required by the Contractor as identified by CBP Field Support.

All required travel shall be performed by the Contractor in accordance with existing Federal Travel Regulations, and with prior (advance) written (email is acceptable) approval from the COTR.

## **12 PERIOD OF PERFORMANCE**

The period of performance for this effort is 5/19/2010 through 11/30/2010.

DHS/CBP personnel observe the following days as holidays:

New Year's Day	Labor Day
Martin Luther King's Birthday	Columbus Day
Presidents' Day	Veterans' Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

Any other days designated by Federal statute, by Executive Order or by the President's proclamations. When any such day falls on a Saturday, the following Monday is observed. Observance of such days by Government personnel shall not be cause for an extension to the delivery schedule or period of performance, or adjustment to the price of this contract, except as set forth in the terms and conditions of the contract.

Except for designated around-the-clock or emergency operations, Contractor personnel will not, without written consent from the COTR, be able to perform work in the CBP facilities. The Contractor will not charge any holiday as a Direct or Indirect Cost. In the event that the Contractor's personnel work during a holiday other than those above, no form of holiday or other premium compensation will be reimbursed as either a direct or indirect cost.

If not emergency-related contractors: In the event DHS/CBP grants administrative leave to its Government employees, Contractor personnel working in the DHS/CBP facilities shall also be dismissed if the facilities are being closed. In each instance when the facility is closed to

Contractor personnel as a result of inclement weather, potentially hazardous conditions, explosions, or other special circumstances; the Contractor shall direct its staff as necessary to take actions, such as reporting to its own facilities or taking appropriate leave consistent with its internal company policies.

Tasks related to this order are to stop at Close of Business on the last day of the period of performance unless contacted by a Contracting Officer, or unless terminated at an earlier date.

The labor under this Statement of Work is subject to the Service Contract Act of 1965.

### **13 STANDARD CLAUSES**

See Addendum B.

### **14 CONTRACTOR EMPLOYEES**

#### **14.1 KEY PERSONNEL**

The Contractor shall notify the Contracting Officer (CO) and the COTR prior to making any changes in the Key Personnel. No changes in Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the Key Personnel being replaced. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The CO and COTR shall be notified in writing of any proposed substitution at least fifteen (15) days, or thirty (30) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include:

- an explanation of the circumstances necessitating the substitution;
- a complete resume of the proposed substitute; and
- any other information requested by the CO or the COTR to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The CO and the COTR will evaluate all substitutions. These individuals will evaluate such requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor. In the event that a change in key personnel is caused by an individual's sudden illness, death, or termination of employment, the Contractor shall promptly notify the CO and the COTR, and provide the information required.

DHS/CBP requires that the contractor provide a Program Manager for this contract and that the Program Manager be designated as Key Personnel. The Program Manager will serve as a point of contact for the COTR and will serve as the interface between the government and the contractor employees. The Program Manager will provide centralized administration of all work performed under this contract.

#### **14.2 PERSONNEL RELEVANT KNOWLEDGE, ABILITIES, AND SKILLS.**

The following is to inform potential contractors of the breadth and scope of skills that CBP may seek under this contract. CBP does not require the Contractor to establish these skill categories as labor categories.

Personnel assigned to perform on this Statement of Work shall be required to possess a diverse set of skills. The labor categories shown in the paragraphs below are those that may be acquired in support of this effort. All personnel performing under this Statement of Work shall be able to perform the duties for their respective Government labor category positions described herein. CBP reserves the right to determine whether an individual's background and experience are sufficient to ensure adequate performance of this effort. All Contractor personnel shall be performing duties at: 1) a Government site, 2) via telework from employee home at on-site rates, or 3) at a Contractor site at contractor off-site rates. CBP shall approve all performance locations, as well as reserving the right to choose the locations.

CBP is not restricting itself to acquiring only the labor categories listed in this document. More precisely, this is not an all-inclusive list of the support, which may be acquired. Specific education, experience and expertise may be required by the individual CBP program offices.

CBP has high volume, high performance and real-time applications operating in an environment that requires specialized, demonstrated management and technical expertise, as well as clearable personnel. In accepting Contractor personnel, CBP will place more value on specialized and demonstrated experience. The Contractor shall provide personnel with specialized and demonstrated experience in an environment similar and relevant to the CBP information technology environment. CBP will give consideration to certifications by recognized organizations in the skill area, to continuing education credits by nationally recognized institutions in related areas of study, and to relevant degrees. Progressive, unique, advanced and specialized experience that demonstrates value added qualifications are considered highly desirable. Personnel demonstrating ongoing development of technical expertise and teamwork capabilities are also highly desirable. Additionally, due to the critical mission and operations of the systems being supported, Contractor personnel who hold current (within the last 3 years) Secret and/or Top Secret clearances, or current DHS/CBP Secret and/or Top Secret clearances, are preferable in order to ensure a smooth transition period.

The Contractor is expected to provide certified, trained, and knowledgeable technical personnel according to the requirements of this contract. Therefore, the CBP will not provide or pay for training, conferences, or seminars to be given to contractor personnel in order for them to perform their tasks. If it is determined during the performance of the task order that training, conferences, or seminars not specified in the task order are required, only the CBP Contracting Officer may approve the training as specified in Section 2.3.9 of this document.

#### 14.2.1 Information Technology Field Services Support

Labor Category	Functional Description	Location(s)
----------------	------------------------	-------------

Network Administrators I, II & III Network Analysts	Field IT- LAN Administrator 1	Throughout the United States, Puerto Rico, Canada, Guam, and the Virgin Islands
Network Engineer II & III	Field - Network Administrator I 1	Throughout the United States, Puerto Rico, Canada, Guam, and the Virgin Islands

1 Based on combination of level-of-experience and education.

#### 14.2.2 Network and Security Operations Center, DHS OneNet

It is suggested that all labor categories have a Department of Defense (DOD) SECRET clearance, however key personnel must possess this level of security clearance. Additional security requirements are outlined in Para 11 of this document. The conducting of this level of back ground investigation is solely the responsibility of the Contractor.

<b>Labor Category</b>
Project Manager (1)
Communications Network Manager (3)
Communications/Network Engineer (2)
Systems Engineer (1)

#### 14.3 Technology Service Desk

#### 14.4 Program and Project Management

##### 14.4.1 The Program Manager

The Program Manager shall serve as the senior member of the Contractor team and shall provide technical direction and guidance to all Contractor employees including scheduling, delegation of duties and responsibilities, development and review of all plans and reports. Ensures that all efforts conform to prescribed agency standards and industry best practices; provides advice to team members on problems and ensures that all time schedules are met; ensures adherence to SLC and CM principles; prepares ad hoc progress and/or management reports as required; schedules and participates in peer reviews; ensures that problem reports are documented and closed within a reasonable period of time; prepares and delivers presentations to colleagues, subordinates, and Government representatives as required; and provides input in preparation for all gate reviews, when appropriate.

The Program Manager requires progressive levels of experience and responsibility in this type of required effort and providing solutions in large legacy mainframe and/or distributed system environments. The Program Manager must have experience in design and documenting in-depth plans and integrated schedules; the use of CM and System Lifecycle (SLC) principles; use

project management tools to track progress of the integrated schedules; communicates effectively orally and in writing.

#### **14.5 WORK HOURS**

The Contractor shall typically work 8 hours a day, 5 days a week, but may be required to work beyond this typical schedule. Contractor personnel shall observe a consistent tour of duty of 40 hours per week, Monday through Friday, with core hours from 9:30 A.M. until 3:30 P.M. Any alterations to the work schedule shall be approved by the COTR. Contractor personnel shall be available for weekend and after hours work as directed by the COTR and may be called upon for after-hour emergencies. All Contractor personnel shall be present during core hours.

In some instances, 7x24x365 operations are maintained and Contractors are required to support these schedules.

#### **14.6 OVERTIME**

Contractor personnel may not work more than 40 hours a week without prior approval of the COTR. Approved overtime hours shall be invoiced at the normal hourly rate for this effort.

#### **14.7 IDENTIFICATION BADGES**

Contractor employees shall be required to wear CBP identification badges at all times when working in Government facilities.

#### **14.8 CONTRACTOR IDENTIFICATION**

The Contractor shall ensure that its employees identify themselves as employees of their respective company while working on DHS/CBP contracts. For example, Contractor personnel shall introduce themselves and sign attendance logs as employees of their company, not as DHS/CBP employees. The Contractor shall ensure that their personnel use the following format signature on all official emails generated by DHS/CBP computers:

- Name
- Position or Professional Title
- Company Name
- Supporting the XXX Division/Office
- US Customs and Border Protection
- Phone
- FAX
- Other contact information as desired

#### **14.9 MANDATORY AND OTHER TRAINING**

If directed by the COTR, the Contractor shall take the DHS/CBP mandatory security training. The Contractor is responsible for maintaining records of contracting employees that have taken the security training and providing the COTR with copies of the training certificates.

CBP shall not incur expenses for training contractor personnel. Contractors are expected to have the requisite skill set to complete the task.

#### **14.10 EMPLOYEE CONDUCT**

The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance, and integrity at all times and shall be responsible for their employee's performance or the quality of the employees' services.

##### **14.10.1 Contractor Input and Tracking**

Before receiving facility badges, the Contractor shall require that each employee under the contract has:

- Entered information into the CBP web-based phone system; and
- Provided the COTR with the information required for the CBP Contractor Tracking System.

In accordance with U.S. Customs and Border Protections Security Policy No. OIT SEC 2.16 "OIT Policy for Centralized Contractor Tracking" The Contractor is responsible for ensuring that all on-boarding and separating employees comply with this directive by immediately supplying the Contract Officer's Technical Representative (COTR) with the relevant information required to satisfy this directives requirements.

#### **15 GOVERNMENT POINTS OF CONTACT (POC)**

Contracting Officer:

Bruce Wood

U.S. Customs and Border Protection

(b) (6)

(b) (6)

See Addendum C for COTR and Task Monitor List.

**ATTACHMENT 1 - ACRONYM LIST:**

ACE	Automated Commercial Environment
AD	Active Directory
AES	Advanced Encryption Standard
AIS	Automated Information System
BI	Background Investigation
BOM	Bill of Materials
BPA	Blanket Purchase Agreement
C&A	Certification and Accreditation
CBP	United States Customs and Border Protection
CCO	Communications Center Operations
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CLIN	Contract Line Item Number
CM	Configuration Management
CMS	Call Management System
CO	Contracting Officer
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations Plan
COTHEN	Cellular Over the Horizon Enforcement Network
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off-the-Shelf
CPIC	Capital Planning and Investment Control
CPU	Central Processing Unit
CSIRC	Computer System Incident Response Center
CSO	Chief Security Officer
CT	Computer Telephony
CTI	Computer Telephone Integration
DAA	Decision Approval Authority
DAR	Designated Agency Representative
DCN	DHS Core Network
DHS	Department of Homeland Security
DM	Domain Control
DOD	Department of Defense
DROC	Disaster Recovery Operation Center
EA	Enterprise Architecture
E-CAS	Electronic Call Accounting System
EDMO	Enterprise Data Management Office
EFT	Electronic Funds Transfer
EIT	Electronic and Information Technology
ENTS	Enterprise Networks and Technology Support
EVC	Voice Communications
EVM	Earned Value Management
EVMS	Earned Value Measurement System
EWP	Enterprise Wireless Programs
FAR	Federal Acquisition Register
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act

## CBP Enterprise Network Services Technology

FMG	Financial Management Group
FOIA	Freedom of Information Act
FOUO	For official Use Only
FSSI	Federal Strategic Source Initiative
FTO	Field Technology Officer
FTR	Federal Travel Regulations
GETS	Government Emergency Telecommunications Service
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GOTS	Government of the Shelf
GSA	General Services Administration
HF	High Frequency
HLS	Homeland Security
HSDN	Homeland Security Data Network
IA	Information Assurance
IP	Internet Protocol
ISA	Interconnection Security Agreement
ISA	Interconnectivity Service Agreement
ISDN	Integrate Services Digital Network
ISSB	Information Systems Security Branch
ISSO	Information System Security Officer
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITP	Information Technology Program
LAN	Local Area Network
LMR	Land Mobile Radio
LPO	Local Property Officer
LRC	Long Range Communication
MAC	Moves, Adds, and Changes
MAN	Metropolitan Area Network
MD	Management Directive
MNS	Managed Network Service
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MSP	Managed Service Provider
NCC	Network Communication Center
NDC	National Data Center
NDS	Novell Directory Services
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NLECC	National Law Enforcement Communications Center
NMT	Network management Team
NSO	Network and Security Operations Center
OAST	Office on Accessible Systems and Technology
ODC	Other Direct Costs
OF	Office of Finance
OIs	Operating Instructions
OIT	Office of Information and Technology
OJT	On the Job Training
OMB	Office of Management and Budget
OneNet	DHS Single Network Project

OR&R	Office of Rules and Regulations
ORR	Operational Readiness Reviews
OTAR	Over the Air Re-key
OTM	The On-Site Task Manager
P25	Project 25
PBX	Private Branch Exchange
PDA	Personal Data Assistant
PE	Provider Edge
PICS	Password Issuance Control Systems
PKI	Public Key Infrastructure
PMBOK	Project Management Body of Knowledge
PMR	Program Management Review
PO	Purchase Order
POA&M	Plan of Action and Milestone
POP	Points of Presence
PR	Purchase Requisition
PRR	Production Readiness Reviews
PSR	Project Status Review
PTP	Point to Point
QoS	Quality of Service
RCA	Root Cause Analyses
RCC	Remote Console Controller
RF	Radio Frequency
RFI	Request for Information
RGV	Rio Grand Valley
RRB	Ronald Reagan Building
SCI	Sensitive Compartmented Information
SDLC	Systems Development Life Cycle
SELC	Systems Life Cycle
SLA	Service Level Agreements
SLO	Service Level Objectives
SME	Subject Matter Expert
SOC	Security Operations Center
SOP	Standard Operating Procedure
SOW	Statement of Work
ST&E	Security Test and Evaluation
TACCOM	Tactical Communication Project
TD	Temporary Duty
TEM	Telecom Expense Management
TO	Task Order
TO-COTR	Task Order Contracting Officer's Technical Representative
TOD	Technical Operations Division
TPOCs	Technical Point of Contact(s)
TRM	Technical Reference model
TSD	Technology Service Desk
TTPs	Tactics Techniques Procedures
TTY	Teletypewriter of Teletype
VoIP	Voice over Internet Protocol
VPN	Virtual Private Networking
VTC	Video Teleconferencing

PR 2005-4702  
CBP Enterprise Network Services Technology

WAN	Wide Area Network
WBS	Work Breakdown Structure
WMP	Wireless Maintenance and Procurement Branch
WNSO	Wireless Network Operation Center
WSOC	Wireless Secure Operation Center

**ATTACHMENT 2 - FIELD SUPPORT APPROVED SOP LIST**

Body Armor  
LAN & Equipment Room Property Transfer Agreement  
Maintenance of Service Provided Equipment in Aircraft  
Remedy RVS Instructions for Field Support  
Travel  
Advance Notification of Work to be Performed  
Awards  
Obtaining New Site Lease  
Purchase Cards  
Reporting Injuries  
Reporting Misconduct  
Space Acquisition  
Visitor Procedures  
Professional Practices  
Labor Employee Relations Procedures  
Fall Protection Program  
Tower Climbing  
Vehicle Management

**ADDENDUM A      POLICIES**

<b>DHS, CBP Policy:</b>	
DHS Earned Value Guidance	Version 1.0, November 2006
CBP System Lifecycle Handbook	Version 1.1, September 2007
OIT Project Management Guidebook	Version 2.0, October 27, 2006
OIT Change Management Handbook	June 1, 2008
OIT Configuration Management (CM) Plan	April 24, 2008
OIT Change Management Policy	June 1, 2007
<b>CBP Information Systems Security Policies and Procedures Handbook 1400-05C</b>	<b>Version 2.1, October 18 2006</b>
CUSTOMS DIRECTIVE NO. 5510-030	Investment Management Process (IMP) Policy
Information Technology Integration and Management	DHS MD 0007.1
Information Security Handbook	DHS 4300
Secure Remote Access Form Completion Process	November 2008
<b>Federal Policy, Laws and Regulations:</b>	
OMB Circular A-130	Management of Federal Information Resources
OMB Circular A-11, Part 7	Exhibit 300
Facilities Standard for Public Building Service	PBS-100
NIST Guide for the Security Certification and Accreditation of Federal Information Systems	SP-B800-37
FIPS Minimum Security Requirements for Federal Information and Information Systems	FIPS-200
FIPS Standards for Security Categorization of Federal Information and Information Systems	FIPS-199
Federal Acquisition Regulation	Part 39, "Acquisition of Information Technology"
Federal Information Security Management Act of 2002	FISMA
Clinger-Cohen Act of 1996 (Public Law 104-106) relating to Capital Planning and Investment Control (CPIC) of Information Technology	
NDIA Earned Value Management Intent 4 Guide	January 2006

NDIA Surveillance Guide	October 2004
40 CFR (all parts)	Code of Federal Regulations, Protection of the Environment (latest version)
Executive Order 12144	Environmental Effects Abroad of Major Federal Actions
Executive Order 13148	Greening of the Government through Leadership in Environmental Management
Executive Order 13101	Greening of the Government through Waste Prevention, Recycling, and Federal Acquisition
Council on Environmental Quality (CEQ) regulations	Latest version
National Environmental Policy Act (NEPA)	Latest version
Industry Standards:	
ANSI/EIA-748	Earned Value Management Systems
ANSI/EIA 748-98	NDIA Earned Value Management Intent Guide and Surveillance Guide
Project Management Institute	Project Management Body of Knowledge

## **ADDENDUM B      STANDARD TERMS AND CONDITIONS**

### **PERIOD OF PERFORMANCE**

- Base: May 19, 2010 thru November 30, 2010

### **EA (Enterprise Architecture) Compliance**

The Offeror shall ensure that the design conforms to the DHS and CBP enterprise architecture (EA), the DHS and CBP technical reference models (TRM), and all DHS and CBP policies and guidelines as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA) such as the CBP Information Technology Enterprise Principles and the [DHS Service Oriented Architecture - Technical Framework](#).

The Offeror shall conform to the federal enterprise architecture (FEA) model and the DHS and CBP versions of the FEA model as described in their respective EAs. Models will be submitted using Business Process Modeling Notation (BPMN 1.1, BPMN 2.0 when available) and the CBP Architectural Modeling Standards for all models. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal technology insertion process which includes a trade study with no less than four alternatives, one of which shall reflect the status quo and one shall reflect multi-agency collaboration. The DHS/CBP TRM/standards profile will be updated as technology insertions are accomplished.

All developed solutions shall be compliant with the HLS (Homeland Security) EA (Enterprise Architecture).

All IT hardware or software shall comply with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model. Submittal shall be through the CBP Data Engineering Branch and CBP EA.

In compliance with OMB mandates, all network hardware provided under the scope of this Statement of Work and associated Task Orders shall be IPv6 compatible without modification, upgrade, or replacement.

### **OAST (Office on Accessible Systems and Technology) 508 Compliance**

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified.

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

**36 CFR 1194.22** – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as Flash or Asynchronous JavaScript and XML (AJAX) then “1194.21 Software” standards apply to fulfill functional performance criteria.

**36 CFR 1194.23** – Telecommunications Products. This applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured or developed or used by the Federal Government.

**36 CFR 1194.24** – Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation has user controls available.

**36 CFR 1194.25** – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement. Specifically but not limited to items using biometrics as described in this work order shall apply with this requirement as well as any other technical standard involving the use of software or Web based interfaces.

**36 CFR 1194.26** – Desktop and Portable Computers, applies to all desktop and portable computers that are procured or developed under this work statement.

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

**36 CFR 1194.41** – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional Performance Criteria”, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY. Exceptions for this work statement have been determined by the Department of Homeland Security. Only the exceptions described herein shall be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS Management Directive (MD) 4010.2. DHS has identified the following exceptions that may be applied:

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

**36 CFR 1194.3(b)** – Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those Contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

## **ISO (Information Security) COMPLIANCE**

- **Information Security Clause**

"All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, *Information Technology Systems Security Program* and *4300A Sensitive Systems Handbook*."

- **Interconnection Security Agreements**

Interconnections between DHS and non-DHS IT systems shall be established through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have signatory authority.

- **System Security documentation appropriate for the SDLC status.**

Security Certification/Accreditation

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with the current version of the DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05, and all applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series). During all SDLC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools. An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, the System Owner is always responsible for information system security (4300A). System owners shall include information security requirements in their capital planning and investment control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS information system. System owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

Disaster Recovery Planning & Testing – Hardware

If the system owner requires a robust DR solution (full redundancy and failover capabilities (for near zero downtime)) then the funded DR solution must match the production environment like-for-like. This solution would also include additional software licenses, hardware, firmware and storage for the DR environment.

The system owner or program office must also include travel, per diem and approximately 16 over the core hours for travel to recovery facilities twice per fiscal year for system administrators, DBA's, end users or testers

If the system owner requires a moderate DR solution that would provide a working environment that is capable of handling their mission essential functions then they can fund a scaled down solution which should still take into consideration additional hardware, software licenses, and storage for the DR environment.

The system owner or program office is still responsible for the costs associated with testing their DR solution; however, for a scaled down solution, it may be possible to leverage or share staff already designated to participate in DR activities.

If the system owner only requires a low DR solution then the system owner or program office can use internal resources to perform a table-top exercise, which generally does not require travel, additional hardware or software licenses.

- **Monitoring/reviewing contractor security requirements clause**

Security Review and Reporting

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, Office of Inspector General, the CBP Chief Information Security Officer, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary 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 DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

- **Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information**

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems*  
Page 98 of 102

*Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

- **OMB-M-07-18 FDCC/Common Security Configuration Clause**

In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at <http://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

## **PERSONNEL SECURITY**

### Security Requirements:

The Contractor shall comply with administrative, physical and technical security controls to ensure that the Government's security requirements are met. During the course of this task order, Contractor shall not use, disclose, or reproduce data, which bears a restrictive legend, other than as required in the performance of this SOW.

### Personnel Security Background Data.

All personnel employed by Contractor and/or responsible to Contractor for work performed hereunder shall either currently possess or be able to favorably pass a full field five (5) year background investigation required by Department policies and procedures for employment. This policy applies to any new personnel hired as replacement(s) during the term of this task order.

The information must be correct and reviewed by the designated Security Official for completeness. Normally, information requested for a background investigation consists of SF-85P, "Questionnaire for Public Trust Positions" or SF-86, "Questionnaire for Sensitive Positions (For National Security)" TDF 67-32.5, "U.S. USCS Authorization for Release of Information", FD-258, "Fingerprint Chart" and a Financial Statement. Failure of any task order personnel to successfully pass a background investigation shall be cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined and approved by the CO/COTR/Task Monitor. This policy also applies to any personnel hired as replacements during the term of the SOW.

The Contractor shall ensure designated key NSO staff maintain a minimum Department of Defense (DOD) SECRET clearance. NSO personnel supporting the Security Operations Center, to include CLASSIFIED and COMSEC tasks, shall also possess or shall be able to obtain a Top Secret Single Scope Background Investigation clearance with Sensitive Compartmented Information (SCI). Upon award and when applicable, the DHS assigned COTR of record shall be responsible for processing the "Department of Defense, Contract Security Classification Specification (DD254)" on behalf of the Contractor. The DD254 will authorize the Contractor to

conduct additional background investigations for assigned task order personnel required to access SCI facilities and/or classified National Security information and applies to any and all personnel hired as replacements during the term of the task order. Background investigations are taking approximately six (6) months from initial acceptance of the security package.

Contractor shall immediately notify the CO and COTR of any personnel changes. Written approval and confirmation is required for phone notification. This includes, but is not limited to, resignations, terminations, and reassignments.

Contractor is responsible for ensuring that task order employees separating from the agency complete the appropriate documentation. This requirement covers all task order employees who depart while the SOW is still active (including resignation, termination, etc.) or upon final completion of this SOW. Failure of a contractor to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

The contractor shall submit within ten (10) working days after award a list containing the full name, social security number, and date of birth of those people who shall require background investigation by the Department, and submit such information and documentation as may be required by the Government to have a BI performed. The information provided must be correct and reviewed by the contractor for completeness. Failure of any contractor personnel to pass a BI shall be cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined and approved by the COTR. This policy also applies to any personnel hired as replacements during the term of the contract.

Contractor shall notify the COTR and the Department of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to another task order. The Contractor/Engagement Manager is responsible for the completion and timely submission to the COTR of appropriate documentation for all departing task order personnel.

## **Portfolio Review**

### **Infrastructure**

Includes all activities related to the planning, design, and maintenance of an IT Infrastructure to effectively support automated needs (i.e., platforms, networks, servers, printers).

#### **Alert/Disaster Management**

Includes all activities needed to prepare for, mitigate, respond to, and repair the effects of natural or man-made disasters; including incident management, and the creation and distribution of alerts, warnings and notifications.

#### **Call Centers**

Includes all activities providing assistance to customers regarding services and benefits, and with issues related to routine administration of citizen services through Electronic Government (e-Gov).

**COOP (Continuity of Operations)**

Includes all activities associated with the identification of critical systems and processes, and the planning and preparation required to ensure that these systems and processes will be available in the event of a catastrophic event.

**Screening/Watch list/Credentialing**

Includes all activities that support the tracking and monitoring of travelers, conveyances and cargo crossing U.S. borders, and traffic pattern analysis, database (Federal, State, and Local) linking and querying, and managing status verification and tracking systems. Different investments and systems may support distinct screening and watch list activities for people, cargo, and tangible goods. Credentialing encompasses all activities that determine a person's eligibility for a particular license, privilege, or status, from application for the credential through issuance, use, and potential revocation of the issued credential.

**Security/Clearance Management**

Includes all activities that protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Also includes all activities that provide physical protection of an organization's personnel, assets, and facilities (including security clearance management).

**ADDENDUM C      COTR AND TASK MONITOR LIST**

**COTR**

(b) (6)

U.S Customs and Border Protection  
7681 Boston Blvd  
Rm 203 C-97  
Springfield, VA 22153

(b) (6)

(d) (v)

**Task Monitor (Field Support Program)**

(b) (6)

U.S Customs and Border Protection  
7681 Boston Blvd  
Springfield, VA 22153

(b) (6)

(d) (v)

**Task Monitor (Network and Security Operations Center)**

(b) (6)

U.S. Customs and Border Protection  
7681 Boston Blvd  
Springfield, VA 22173

(b) (6)

(d) (v)

**Task Monitor (Technology Help Desk)**

(b) (6)

U.S. Customs and Border Protection  
7501 Boston Blvd  
Springfield, VA 22153

(b) (6)

(b) (6)

**Task Monitor (Information Technology Program)**

(b) (6)

U.S. Customs and Border Protection  
7451 Boston Blvd  
Springfield, VA 22153

(b) (6)

(d) (v)