

DATE OF ORDER 05/22/2007	CONTRACT NO. (if any) HSHQDC06D00024	ORDER NO. HSBP1007J15141	PAGE OF PAGES 2 3
-----------------------------	---	-----------------------------	----------------------

Federal Tax Exempt ID: 72-0408780

NOTES:

This Labor Hour type task order (HSBP1007J15141) is issued against the Department of Homeland Security's (DHS) Enterprise Acquisition Gateway for Leading-Edge Solutions (EAGLE) contract, under contract number HSHQDC-06-D-00024. All terms and conditions of both the Customs and Border Protection (CBP) task order and the EAGLE contract are in full force and effect.

This task order is issued for Security Support Services in the Security Operations Center of the Office of Information Technology, in accordance with the attached Statement of Work (SOW) and General Dynamic's Price Proposal dated April 20, 2007.

The SOW and Price Proposal are hereby incorporated into this task order.

The Base Period of Performance for this task order is July 1, 2007 through June 30, 2008.

Line items 10, 20 and 30 in the combined total amount of (b) (4) are for labor.

Line item 40 in the amount of (b) (4) is for travel.

The Ceiling Price for the Base Period is \$6,501,230.40.

All labor rates are fixed unit prices.

All travel is a cost reimbursable line item. All travel shall be billed in accordance with the Federal Travel regulations.

Option Year I Period of Performance:

July 1, 2008 through June 30, 2009

Estimate: (b) (4)

((b) (4) for labor and \$(b) (4) for travel)

Option Year II Period of Performance:

July 1, 2009 through June 30, 2010

Estimate: (b) (4)

((b) (4) for labor and (b) (4) for travel)

Option Year III Period of Performance:

July 1, 2010 through June 30, 2011

Estimate: (b) (4)

((b) (4) is for labor and (b) (4) is for travel)

Option Year IV Period of Performance:

July 1, 2011 through June 30, 2012

DATE OF ORDER 05/22/2007	CONTRACT NO. (if any) HSHQDC06D00024	ORDER NO. HSBP1007J15141	PAGE OF PAGES 3 3
-----------------------------	---	-----------------------------	----------------------

NOTES:

Estimate: (b) (4)
(b) (4) is for labor and (b) (4) is for travel)

The total ceiling amount of this task order is (b) (4) (Base Period plus 4 Option Years).

(b) (6) is the designated Contracting Officer's Technical Representative (COTR) for this Task Order.

Please submit all invoices to each of the following:

US Customs and Border Protection
Attn: (b) (6)
7681 Boston Boulevard, NDC1, Rm 2014
Springfield, VA 22153

-and-

DHS- Customs and Border Protection National Finance Center (Address in section 17 of this task order)

Attachments: SOW, Clauses, and Accounting Data.

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: HSBP1007J15141**

SCHEDULE OF SUPPLIES/SERVICES

Item Number:	00010	Line Item (Priced/Information/Option):	P	
Supplies/Services:	Security Operations Center Labor			
	Qty	Unit	Unit Price	Ext. Price
	1	AU	\$(b) (4)	(b) (4)
Item Number:	00020	Line Item (Priced/Information/Option):	P	
Supplies/Services:	Security Operations Center Labor			
	Qty	Unit	Unit Price	Ext. Price
	1	AU	(b) (4)	(b) (4)
Item Number:	00030	Line Item (Priced/Information/Option):	P	
Supplies/Services:	Security Operations Center Labor			
	Qty	Unit	Unit Price	Ext. Price
	1	AU	(b) (4)	(b) (4)
Item Number:	00040	Line Item (Priced/Information/Option):	P	
Supplies/Services:	Security Operations Center Travel			
	Qty	Unit	Unit Price	Ext. Price
	1	AU	(b) (4)	(b) (4)
Item Number:	00050	Line Item (Priced/Information/Option):	O	
Supplies/Services:	Security Operations Center Option 1			
	Qty	Unit	Unit Price	Ext. Price
	1	AU		(b) (4)
Item Number:	00060	Line Item (Priced/Information/Option):	O	
Supplies/Services:	Security Operations Center Option 2			
	Qty	Unit	Unit Price	Ext. Price
	1	AU		(b) (4)
Item Number:	00070	Line Item (Priced/Information/Option):	O	
Supplies/Services:	Security Operations Center Option 3			
	Qty	Unit	Unit Price	Ext. Price
	1	AU		(b) (4)
Item Number:	00080	Line Item (Priced/Information/Option):	O	
Supplies/Services:	Security Operations Center Option 4			
	Qty	Unit	Unit Price	Ext. Price
	1	AU		(b) (4)
Total Funded Contract Value:				<u>\$6,501,230.40</u>

ACCOUNTING AND APPROPRIATION INFORMATION

Item: 00010 6100.2525USCSGLCS0923020314Z00007164HQ01 IR1462525 Amount \$(b) (4)

Item: 00020 6100.2525GLCS0923020314ZJ7W07074R0HQ01 IR1462525 Amount (b) (4)

Item: 00030 6100.2525GLCS0923020314ZJ6Q06061R0HQ01 IS4502525 Amount (b) (4)

Item: 00040 6100.2525USCSGLCS0923020314ZJ7W07074R0HQ01
IR1462525 Amount (b) (4)

DELIVERY SCHEDULE

Deliver To: Customs and Border Protection
7681 Boston Blvd
VA95 Bus Pk
Springfield VA 22153

Instructions: Item	Quantity	Delivery Date	Recipient	Unloading PT.
00010	1	06/30/2008		
00020	1	06/30/2008		
00030	1	06/30/2008		

=====

Deliver To: Customs and Border Protection

7681 Boston Blvd.
VA95 Bus Pk
Springfield VA 22153

Instructions:

Item	Quantity	Delivery Date	Recipient	Unloading PT.
00040	1	06/30/2008		



STATEMENT OF WORK
For

Security Support Services
US Customs and Border Protection
Security Operations Center

March 5, 2007

~~Limited Official Use~~

1.0 OVERVIEW AND BACKGROUND

The United States Customs and Border Protection (CBP) is one of 22 Department of Homeland Security (DHS) federal agencies. The CBP mission is to protect our Nation's borders from terrorist attacks, to enforce the laws of over forty agencies and to protect the revenue of the United States while facilitating trade. Losing the capability to process, retrieve and protect electronic data can significantly harm CBP's ability to accomplish its mission. The mission of the CBP Security Operations Center (SOC) is to coordinate department level support to ensure the security of DHS information systems. The SOC operations range from computer security incident response to security device configuration, event monitoring, alerts analysis, and preventive measures.

The CBP SOC was established in accordance with the Federal Information Security Management Act (FISMA 2002), and the Homeland Security Presidential Directive, HSPD-7. The SOC is chartered to prevent, detect, contain, and eradicate security threats from the CBP network. The CBP SOC provides monitoring, intrusion detection, and protective security services to assigned information systems, to include wide area network (WAN) and local area network (LAN) security devices, application servers, and workstations. The SOC is responsible for the overall security of Enterprise-wide information systems, and collects, investigates and reports any suspected and confirmed security violations.

DHS has designated the CBP SOC as the Steward Agency for Network Services and Data Center Services. The "Department of Homeland Security Information Technology Program Interim Management Directive, MD 4300A, Volume I Policy, Part 1 Sensitive Systems, Section 4.10.1 Security Incident and Violation Handling" provides the policy basis for the services outlined in this document. The services offered by the DHS SOC are available only to DHS Component agencies, computer systems and LAN segments connecting directly to the DHS core, and DHS locations and personnel using DHS furnished equipment both within the United States and abroad. There are approximately seven subordinate SOCs in the DHS, and as the Steward, CBP SOC has a need to track the reportable security incidents as the centralized coordination point of contact. The SOC performs event tracking using an automated system, provides security expertise, event coordination and response using leading-edge technologies, collection techniques, and Commercial Off The Shelf (COTS) applications and products. The SOC manages and maintains SOC operations using approved security devices as documented in the DHS Technical Reference Model (TRM).

2.0 OBJECTIVE

The objective of this task order is to acquire services to manage, operate and maintain the CBP SOC to accomplish the DHS Stewardship security operations mission. The Contractor shall support continuous 24x7 managerial, technical, and operational SOC

support to the DHS WAN and integrated Component agency LAN networks. The Contractor must coordinate Department-level incident response and identify, report, and manage the resolution of computer security irregularities that affect DHS's ability to conduct its mission.

3.0 SCOPE OF WORK

The Contractor shall provide security services support to the CBP SOC, to include, but not limited to, the DHS WAN environment, also known as "DHS OneNet", its data centers, and integrated Component LANs. The SOC is a 24x7 center that operates in the confines of a secure facility, organized, staffed, and equipped to manage security specific functions that have relevance across an enterprise. In addition, the Contractor shall provide for security services to other DHS Components and coordinate activities with the Component agency SOCs. Basic Services provided include network and application layer monitoring and analysis, computer security incident response, and vulnerability assessment. Additional services include host-based antivirus protection, patch management, penetration testing and computer forensics. These services and expected level offerings are defined in more detail in this SOW section 4. This contract is based on an annual basis from date of award with (4) option years dependent upon the availability of funds and satisfactory performance.

4.0 GENERAL REQUIREMENTS

4.1 TASK 1: MONITORING AND ANALYSIS

4.1.1 General Requirements

The Contractor shall provide 24x7x365 skilled security personnel that shall provide continuous monitoring, analysis and reporting of security alerts information from all approved security devices, collection techniques and designated system logs. The monitoring and analysis shall consist of, as a minimum, security event detection, categorization, prioritization and reports. The event categorization shall consist of analysis of the incoming data flow from security devices and searching data for indications of anomalous events. The Contractor shall provide technical staff to investigate anomalous events that are detected by security devices or reported to the SOC from external entities, DHS Components, system administrators, and the user constituency via incoming phone calls, emails, and the CBP Technical Support Center (TSC) trouble ticket system. The Contractor handling of security events shall be logged, recorded, and reported.

The SOC serves as an escalation center and as the central coordination point of contact for computer security incidents across DHS. The Contractor shall provide notification and daily summary reports based on security event analysis. The Contractor shall configure and manage security tools to optimize data correlation and event discovery and detection. The Contractor shall devise test plans and recommend upgrades to automated security tools to prevent, monitor and assess the status of the DHS OneNet wide area network, data centers, and Component level LANs. The Contractor shall manage the resolution of computer security events that affect DHS information systems through the use of an established ticketing system. The Contractor shall ensure that refresher training is provided to their staff to maintain the staff's level of competency.

4.1.2 Monitoring and Analysis Subtasks

4.1.2.1 Security Event Categorization

The Contractor shall furnish technical expertise to monitor and analyze security event data to include investigation of reported incidents using system logs, event correlation between Intrusion Detection Systems (IDS) and firewalls. The monitoring and analysis shall also include data and results of vulnerability scanning, patch management, anti-virus devices and management, host-based and network based IDS and Intrusion Prevention Systems (IPS), and network security compliance health monitoring. The Contractor shall review audit logs and record any inappropriate or illegal activity in order to reconstruct events during a security malfunction. As required, the Contractor shall use Government approved automated tools, collect scripts, or digital forensics techniques to collect additional data for event analysis. The Contractor shall provide event analysis and evaluation of the reported violation and provide post-analysis categorization, prioritization, and recommendation of event disposition. The Contractor shall document all event investigation activities, incoming requests for information, or suspected incident reports as required to support law enforcement records, case disposition and audit review.

4.1.2.2 Security Event Notification

The Contractor shall provide notification, and as needed, escalation of security events to initiate containment activities. All problems will be escalated and reported in accordance with DHS Policy and established reporting timelines. The security event notification shall include security recommendation, technical guidance and coordination for the overall approach for the containment and eradication of the security event.

Due to the complex nature of the DHS IT infrastructure, it is possible for the source of a problem or incident to reside in one or more areas concurrently. As such, the Contractor shall perform troubleshooting techniques to isolate the source of, diagnose, and resolve or assist in the resolution of network security-related incidents. The Contractor shall maintain a current listing of Department and Component and relevant external entities points of contacts and will update the list periodically to assure its accuracy.

4.1.2.3 Security Tool Configuration

The Contractor shall provide for in-house administration, management, and configuration

of the SOC tools, devices and application systems, dedicated servers and sensors. The Contractor shall review network security architecture and design and provide security device signature maintenance and performance reports. The Contractor shall maintain the Security Information Manager (SIM) to collect and aggregate IDS data from network sensors, raw data from collection agents, firewalls, antivirus, and vulnerability scanner elements. Emerging trends and authorized security tools shall be under continuous test and evaluation to remain current with the DHS network architecture. To assist the Contractor in identifying, analyzing and defining network security-related problems, the Government shall provide to the Contractor access to the use of a wide assortment of diagnostic and monitoring tools. The Contractor shall select the diagnostic tool or monitoring tools that are appropriate for use in diagnosing problems. The Contractor shall also recommend tools to enhance or replace existing tools in the DHS TRM.

The Contractor shall install or modify network security components, tools, and other systems as required to maintain optimal coverage and performance. Any configuration changes shall be documented using the approved change management (CM) process and procedures. The Contractor shall provide a list of all newly installed Government owned equipment and software for input into the TRM and the Infrastructure Information Repository (IIR), which is the approved DHS design database.

The Contractor shall assist in the tracking and management of the SOC security devices, physical property, asset management and any Government Furnished Equipment (GFE) provided to the Contractor to perform its duties. The Contractor shall provide, as collateral duties, a Local Property Officer (LPO) and Inventory taker assignments for the SOC to document property and inventory. The Contractor shall document software licenses, and track maintenance and support agreements.

4.1.3 Monitoring and Analysis Reports

The Contractor shall provide written reports detailing all security events relative to network security matters and submit these reports according to established procedures and reporting requirements. The Contractor documentation of incident investigation and case analysis shall be in accordance with approved law enforcement collection and documentation techniques, and be able to support chain of custody and digital forensics requirements.

The Contractor shall use the trouble ticket system to take appropriate action towards problem status documentation, resolution and prevention measures. The Contractor shall also provide information to impacted users and management promptly regarding the status of changes, enhancements, and problem resolution. The Contractor shall complete resolution or referral of all network security problems after receiving notification of an incident or problem in accordance with established timelines (see Appendix A: Service Level Objectives). The Contractor shall provide summary of ticket system activities.

4.2 TASK 2: COMPUTER SECURITY INCIDENT RESPONSE CENTER (CSIRC)

4.2.1 General Requirements

The Contractor shall provide skilled technical and security expertise to conduct coordinated computer security incident management and response to meet reporting requirements of FISMA, other National directives and DHS Policy. The Contractor shall support the DHS Computer Security Incident Response Center (CSIRC) as well as conduct research into the threat environment, assess the situation, and determine relevance to the DHS environment and provide security situational awareness. The DHS CSIRC is a function within the DHS SOC and is the central repository and coordination point for all of DHS computer security incidents. The DHS CSIRC provides technical assistance, advises Components CSIRCs or subordinate SOCs, and facilitates two-way information sharing. The CSIRC management and response operations coordinate DHS-wide incident reporting and response to incidents escalated from the DHS SOC analysts, the Network Operations Center (NOC), subordinate and Component SOCs, system administrators, and the constituency. The National Information Security Technology (NIST) Special Publication (SP) 800-61 Computer Security Incident Handling Guide, describes the guidelines employed by DHS CSIRC in handling adverse events and incidents. The CSIRC operates synergistically with the DHS Office of the Chief Information Operations (OCIO) and Chief Information Security Officer (CISO) on committees and workgroups pertaining to incident response, emergency response, other SOC/CSIRC related activities, and DHS mandated directives. The Contractor shall develop and maintain formal, documented and approved, incident response procedures, DHS to Component SOC Concept of Operations (ConOps) and reporting guidelines.

4.2.2 CSIRC Subtasks

4.2.2.1 Centralized DHS Security Incident Management

The Contractor shall provide DHS CSIRC services as the central point of contact for all computer-related security incidents, as well as security reporting to keep the DHS leadership informed of matters concerning the security of the DHS OneNet. The Contractor shall coordinate and oversee the DHS incident and outage escalation process. The Contractor shall provide DHS Components specific information security bulletins, alerts, and technical advisories. The CSIRC shall maintain a database of all reported incidents to provide mandated routine and situational reports to other agencies to meet FISMA requirements. The Contractor shall establish routine communication mechanisms, daily status call, incident-specific conference calls, retrievable, customized on-line reports, and email and ticket notifications to share relevant information with other DHS SOCs and Components' Information System Security Managers (ISSMs). The Contractor shall coordinate with other DHS entities, to include, but not limited to, the U.S. Computer Emergency Response Team (US CERT), the DHS Office of Security (OSC), law enforcement officials, the Office of the Inspector General (OIG), and the National Operations Center (NOC). As required, the Contractor shall provide DHS representation to external Government Agencies and National Security forums and discussions.

4.2.2.2 Vulnerability Management Alerts, Advisories and Bulletins

The Contractor in support of the CSIRC shall monitor changes in threats, vulnerabilities, impacts, risks and the environment as relevant to the DHS enterprise and assess the risk to the IT infrastructure and applications. The Contractor shall provide these alerts and advisory bulletins following the established DHS Information Security Vulnerability Management (ISVM) notification program. The Contractor in support of the CSIRC shall provide expertise, leverage SOC tools and methodologies to track DHS-wide Component acknowledgement and compliance of the ISVM alerts, advisories and bulletins. The Contractor shall perform trend analysis to compile longer-term configuration assessments, policy, and architecture recommendations and reports for various network security areas of interest. These reports shall supply both generalized and specific information about targeted areas and shall provide recommendations for improving the overall network security of the DHS Information Technology (IT) infrastructure.

4.3 TASK 3: VULNERABILITY ASSESSMENT

4.3.1 General Requirements

The Contractor shall centrally coordinate DHS enterprise Vulnerability Assessment (VA) and penetration testing activities supporting the SOC Vulnerability Assessment Team (VAT). The VAT has appropriate written authority to oversee technical Vulnerability Assessments carried out on DHS assets, maintain an up-to-date collection of GFE technical security vulnerability tools, and ensure that results from the assessments are made available to the appropriate system owners.

The Contractor shall ensure complete coverage of network, host, and wireless assessments of DHS's networks and information systems through scheduling, planning, coordinating and executing assessments with DHS Components and regional security teams.

4.3.2 Vulnerability Assessment Subtasks

4.3.2.1 Maintain Vulnerability Assessment Tools

The Contractor shall maintain an up-to-date collection of vulnerability assessment tools as part of scheduled automated reviews of technical environments, as part of security test and evaluation, patch management, and to support incident response. To assist the Contractor in identifying, analyzing and defining network security-related problems, the Government will provide to the Contractor access to the use of a wide assortment of diagnostic and assessment tools. The Contractor shall select the diagnostic tool as appropriate for use in diagnosing problems. The Contractor shall recommend tools to enhance or replace existing tools in the DHS TRM.

4.3.2.2. Conduct Vulnerability Assessments

The Contractor shall conduct, operate and maintain assessments and the resultant VA data and reports. The Contractor shall publish regularly scheduled vulnerability

assessments using a master schedule. The Contractor shall coordinate the VA testing in advance with the NOC and the Components SOCs to assure coordination with network maintenance, availability, and operations. The daily scan schedule shall be coordinated with Components on the daily operations status call. The Contractor shall coordinate with system owners any necessary changes to the schedule. The Contractor shall use approved test procedures, information collect scripts, and VA tools that are Common Vulnerabilities and Exposures (CVE) database compatible; the latest versions of tools with up-to-date lists of vulnerability checks; appropriate to DHS's policies, needs and technologies.

The Contractor shall conduct specialized VA testing to include but not limited to penetration testing, telephone system testing (also known as "wardialing") and wireless access testing. Specialized testing shall be conducted only under well-defined Rules Of Engagement (ROE). The Contractor shall prepare and submit ROE for managerial approval prior to conduct of penetration testing. The ROE is a formal memorandum of understanding between the affected parties, and is a signed agreement defining and coordinating the VA operating procedures and protocols, usage of the VA tools, testing times, network address space, and lists any exclusions, constraints, analysts permissions, and report disposition. The Contractor shall ensure the ROE provides the operational security controls to protect both the system and network.

The Contractor shall be authorized to employ ad-hoc or emergency VA testing to support incident investigation, escalation and emergency response to security events in accordance with documented procedures. The VA will include, but is not limited to tests against specific operating systems (OS), major applications, hosts, network resources, firewalls, routers, IDS, and wireless systems. The Contractor shall conduct network scanning to map out network topology, determine what ports are open, determine specific OS, major applications, and hardware platform on each host on the network and identify and enumerate any vulnerabilities that exist in the system.

4.3.2.3 Vulnerability Assessment Reports

The Contractor shall provide vulnerability assessment summary reports of the testing and document the findings. The documentation must include summary analysis of findings, impact of finding, and recommendations for fixes or other security mitigation strategies. The Contractor shall archive VA data and reports and use findings in the conduct of follow-on assessments, to compare results, focus on deferential findings, look for evidence or lack of improvements thereof to report trends, determine effectiveness of mitigation strategy, and provide recommendations to changes in DHS Policy or architecture.

4.4 TASK 4: MANAGED SECURITY SERVICES

4.4.1 General Requirements

The Contractor shall provide managed security services offerings to support DHS on a Component subscription basis to include digital forensics, anti-virus support, security

change request and configuration management, and security certification support. It is not the intent of this section to describe all of the security services that may be offered by the Contractor to the SOC, but to provide description of the DHS SOC as a managed security services provider. The following lists the range of SOC services as described in the DHS OneNet Consolidated Charter and the DHS OneNet functional requirements documents. This task shall include, but is not limited to the Contractor providing the following services:

- Computer Security Incident Response and management;
- Event correlation between Intrusion Detection Systems (IDS) and firewalls for early warning, alerting, and trends;
- Firewall management in coordination with the Network Operations Center (NOC); data integrity, confidentiality, and availability;
- Monitoring access control;
- Engineering Change Requests (security review) and Configuration Management;
- Anti-virus support and management;
- Host-based and Network-based Intrusion Detection and Prevention;
- Network security compliance health checking;
- Vulnerability scanning to include penetration testing;
- Vulnerability (patch) management;
- Network and applications security advisory and customer notification;
- Compliance with service level agreements (SLAs);
- Reporting;
- Malicious code corrective measures;
- System security configuration validations;
- Mitigation of network security vulnerabilities;
- User identification;
- Digital forensics;
- Access authorization and administration; and
- Support for charge-back services to other DHS components;

4.4.2 Managed Security Services Subtasks

4.4.2.1 Digital Forensics

The Contractor shall maintain the ability to conduct and support digital forensics activities. This includes establishing policies and procedures to preserve the chain of custody of equipment that will be investigated. It also involves maintaining adequate facilities to store equipment of different classification levels. Lastly, it involves ensuring that appropriate forensic tools and equipment (i.e. spare hard drives for replication) are maintained and the Contractor has personnel that are trained and certified in forensics processes and the specific tools selected.

4.4.2.2 Penetration Testing

The Contractor shall maintain the capability to support penetration testing as requested by

Components or system owners in support of security test and evaluation (ST&E) activities. A penetration test goes beyond identifying exposures, and the test shall attempt to exploit vulnerabilities discovered in a vulnerability assessment. This is pursued in order to additionally measure the impact of the exposures. Penetration testing is also known as red teaming, tiger teaming, or ethical hacking. The Contractor shall conduct penetration testing only under very well defined rules of engagement as described in paragraph 4.3.2.2 on all test security control details to protect both the system and network. The Contractor shall provide a detailed report of the findings and recommendations to the system owner and archive the data to be available to support for remediation activities, retest and comparative analysis.

4.4.2.3 Anti-Virus Support

The Contractor shall maintain Anti-Virus software systems deployed strategically to detect and eradicate known malicious code before infecting OneNet systems. Sensors are deployed at all boundary points and monitor web and email traffic in particular, since these are the most common entry points for the introduction of malicious code. The Contractor shall monitor the virus protection control policy.

4.4.2.4 Engineering Change Request and Security Review

The Contractor shall review DHS OneNet and CBP engineering change requests (CR) and configuration changes as security subject matter experts on the CBP Change Control Board. The Contractor shall attend CCB meetings that directly or indirectly assist in providing CR security review services to the CBP engineering environment and provide security advisement to approve, rework, or deny engineering CRs to the appropriate Branch Director and CCB voting members. The Contractor shall provide justifications and supporting documentation for security advisements, provide recommendations for configuration management, and check for compliance to DHS policy, standards, and hardening guidelines.

4.4.2.5 Certification & Accreditation Support

The Contractor shall provide support to the SOC Certification and Accreditation Process following NIST SP 800-53 to include, but not limited to the following elements:

- System Security Plan;
- Security Risk Assessment;
- Security Test and Evaluation (ST&E);
- Continuity of Operations Plan (COOP);
- Development of Plan of Action and Milestones (POAM); and
- Provide, as collateral duties, a SOC System Information System Security Officer (ISSO) to document and maintain the SOC C&A documentation in the Risk Management Systems (RMS), conduct NIST 800-26 self-assessment and track SOC POAM;

The Contractor shall develop and document a comprehensive continuity of operations plan (COOP), maintain appropriate backups of its own infrastructure, and document priorities and procedures for re-instantiating critical functions in the event of a failure.