The Contractor shall test the COOP in conjunction with internal test procedures and the CBP Disaster Recovery Operations Center.

The Contractor shall provide support to SOC/CSIRC management by establishing a POAM and process for tracking the correction of internal self-assessment external audit findings and any external auditor security assessment findings that relate to certification and accreditation of SOC operations and activities.

5.0 DELIVERABLES AND REPORTING REQUIREMENTS

All deliverables produced as a result of this Task Order shall become the property of the Government. Deliverable format shall be based on the type of document and shall conform to CBP directives, where appropriate, and be consistent with other similar efforts. Deliverables shall be accurate in presentation, technical content and adherence to accepted elements of style. The Contractor shall provide the following deliverables:

5.1 Deliverable Requirements

5.1.1 Project Management Plan

The Contractor shall develop a Project Management Plan for this effort. In the Project Plan the Contractor shall provide the following:

- Specification of activities to be performed, including the sub-tasks listed in this section;
- Detail schedule identifying work activities, deliverable due dates and milestones;
- Resources to be used, including personnel and level of effort; and
- Any other items impacting performance of this task;

The Contractor shall present a Draft Project Plan to the SOC Project Staff and the Onsite Task Monitor (OTM) in a Kick-off meeting to be held within 10 days of contract award.

5.1.2 Performance Metrics

The Contractor shall assist in the development of SOC and CSIRC performance and business metrics for each of the support tasks relating to the SOC. 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 SOC objectives.

5.1.3 Presentations

The Contractor shall prepare presentations, as requested, covering work described in the SOW. These presentations will normally be prepared using Microsoft PowerPoint or as otherwise directed by the OTM.

5.1.4 Standard Operating Procedures

The Contractor shall develop and maintain formal, documented SOC standard operating procedures. The SOP provides the operational basis for the DHS SOC Concept of Operations (ConOps), and SOC Center-to-Center Guidelines, and any Memorandum of Agreement between Component SOCs and the OneNet SOC. The Contractor shall submit the draft SOC SOP for Government review within 20 days of contract award and these procedures will be reviewed and updated on an annual basis from the date of approval.

5.1.5 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 SOC SLOs are listed at Appendix A. As Components subscribe to the DHS SOC services, the Contractor shall develop formal SLOs in a Memorandum of Agreement between the DHS SOC to Component SOC.

5.2 Reporting Requirements

5.2.1 Daily Status Report

The Contractor shall facilitate a daily SOC operational conference call, and provide daily status report to support the DHS OneNet NOC/SOC operations. The Contractor shall submit SOC input to the agenda and updated detailed activity will be provided daily by 1200 pm. Conference call information includes any reported Component security incidents, security event notifications, security device outages, vulnerability advisements, alerts, intrusion detection signatures, and threat bulletins released in the previous 24 hours. This information may be accessed by authorized users to retrieve ad-hoc reports using the DHS SOC 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 SOC report.

The Contractor shall provide the daily SOC security status reports to authorized users to include, but not limited to the DHS and Component Chief Information Officers (CIOs); the DHS CISO, and DHS ISSMs. Information provided to authorized Component-level individuals will be limited to the respective Component data. This information may be accessed by authorized users 24x7 on an ad-hoc reports basis, using the DHS SOC On-Line web portal updated continuously. The Contractor shall provide as a minimum the following information for the daily status report.

- Vulnerability Assessment Schedule
- Vulnerability Assessment Reports
- Intrusion Detection Reports
- Computer Security Incident Reports
- Security Event Notifications
- Security Alerts, Advisories and Bulletins

5.2.2 Weekly Status Reports

The written weekly report shall consist of a summary of all SOC activities and reference analysis of SOC performance metrics, track status security incidents, by category, tickets, call logs, investigatory cases, security event notifications and actions accomplished for the week. This report shall be prepared by the SOC 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.

5.2.3 Monthly Reports

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, 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.

5.3 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 make available to all attendees prior to, or at the time of the briefing.

5.3.1 Kick-Off Meeting/Draft Project Schedule:

A task order kick-off meeting will be scheduled within 10 days after contract award. Attendee will be at a minimum: The COTR, the On-Site Task Manager (OTM), Technical Point of Contact(s) (TPOCs), SOC Project Staff Team Leads and the Contractor Project Manager. The Contractor shall provide a draft schedule of their plan to meet the customer's requirements as identified in this SOW. The schedule will be due 10 days after contract award. Any changes or adjustments to this schedule shall be coordinated with the COTR and appropriate OTM.

5.3.2 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.

5. 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.

5.4.1 Deliverable Requirements Delivery Schedule

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
1	Kick-Off Meeting/Draft Project Schedule	5.3.1	Within 10 days after contract award	COTR will be given 5 business days to review and comment, with Final due 5 business days after COTR comment	OTMs, COTR, SOC Project Staff, Contract Project Manager
2	Project Management Plan	5.1.1	Within 20 days after contract award	COTR will be given 5 business days to review and comment, with Final due 5 business days after COTR comment	OTMs, COTR, Contract Project Manager
3	Project Metrics	5.1.2	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager
4	Standard Operating Procedures	5.1.4	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, applicable OTM
5	Monitoring and Analysis Reports	4.1.3	Within 20 days after contract	Within 30 days after contract award	OTMs, COTR Contractor PM

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
			award		
6	CSIRC Incident reports	4.2.2.1	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, authorized DHS recipients, ISSMs
7	CSIRC Vulnerability Management (ISVM)	4.2.2.2	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, authorized DHS recipients, ISSMs
8	Vulnerability Assessment Reports	4.3.3	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, authorized DHS recipients, ISSMs
9	Engineering Change Request (CR) review	4.4.2.4	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, TPOCs
10	Maintain SOC Certification & Accreditation (C&A) Documentation	4.4.2.5	Within 20 days after contract award	Within 30 days after contract award	OTMs, COTR, Contract Project Manager, authorized DHS recipients, TPOCs
11	Service Level Objectives	5.1.5	As required	As required	OTMs, COTR, Contract Project Manager, authorized DHS recipients, TPOCs

5.4.2 Reporting Requirements Delivery Schedule

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
11	DHS OneNet SOC Daily Status Report	5.2.1	Within 30 days after contract award	Daily	OTMs, COTR, Contract Project Manager, applicable DHS recipients OTM
12	Weekly Reports	5.2.2	Within 30 days	Weekly	OTMs, COTR, Contract Project

			after contract award		Manager, applicable DHS recipients OTM
13	Monthly Reports	5.2.3	Within 30 days after contract award	Monthly	OTMs, COTR, Contract Project Manager, applicable DHS recipients OTM
14	Cost Reports	5.3.2	Monthly	Monthly	OTM, COTR
15	Periodic Meetings	5.3.1	As required	As required	COTR, Applicable OTMs, applicable DHS recipients, OTM

5.5 Acceptance Requirements of Deliverables

5.5.1 General Quality Measures

General quality measures, as set forth below shall be applied to each work product received from the Contractor under the SOW. Specific criteria shall be set forth for each task and expected levels of quality shall be agreed upon in a formal agreement between the Contractor, CBP SOC On-Site Task Monitor and the Component SOC.

Accuracy. Work products shall be accurate in presentation, technical content and adherence to accepted elements of style.

Clarity. Work products shall be clear and concise; engineering terms shall be used, as appropriate. 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 product shall adhere to CBP System Development Lifecycle (SDLC) and DHS-based templates, standards and directives.

File Editing. All text and diagrammatic files shall be editable by the Government.

Format. Work products shall be submitted in media defined in Section 4 Deliverables. The work product format may change from subtask to subtask. 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.

6.0 PERIOD OF PERFORMANCE, ESTIMATED STAFFING, LABOR CATEGORY DESCRIPTIONS AND KEY PERSONNEL

6.1 Periods of Performance

The period of performance shall be from date of award through one year with four (4) option periods of one year each. The potential, therefore, is for this contract to run five years from date of award, ending in 2012. The implementation of the optional periods is dependent upon the availability of funds and satisfactory performance.

6.2 Level of Effort (Project Staffing Estimates)

The Contractor shall provide qualified and experienced technical personnel to support the CBP SOC in accomplishing its mission. The mission of the SOC is identified in the Overview and Background section of this SOW. The Contractor shall ensure that opportunities for cross-utilization and cross training of personnel are maximized. The labor categories below are the interpretation of labor requirements under this Task Order. The stated labor mix in this SOW is suggested however the Contractor is allowed and encouraged to propose an alternate mix. It is suggested that all labor categories have a Top Secret Clearance. However, an active Top Secret Clearance is required for all key personnel at award. The conducting of this level of background investigation is solely the responsibility of the Contractor. The following estimates are for planning, proposal pricing and evaluation purposes:

Labor Category	Estimated Number of FTEs	Hour by Labor Category
Project Manager **(Key Personnel)**	1	1920
IT Security Specialist (Senior) **(Key Personnel)**	2	3840
IT Security Specialist (Senior)	3	5760
IT Security Specialist	10	19200
Jr. IT Security Specialists (Junior)	15	28800
System Developer	1	1920
Web content administrator	2	3840
Technical Writer	1	1920
Systems Engineer **(Key Personnel)**	2	3840

Systems engineer	4	7680
	41	

6.3 KEY PERSONNEL:

- The key personnel specified in section 6.2 are considered essential to the work being performed under this contract. During the first sixty (60) days of the task order, the Contractor shall not make any key personnel changes unless an individual's sudden illness, death or termination of employment necessitates such substitutions. In case of theses occurrences, the Contractor shall notify the Contracting Officer and COTR promptly and submit documentation pertaining to the proposed substitution in writing.

- Before removing or replacing any of the specified individuals, the Contractor shall notify the Contracting Officer Technical Representative (COTR), in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the COTR to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel until the COTR approves the change.

- It is suggested that all labor categories have a Department of Defense (DoD) Top Secret Clearance. However an active Top Secret Clearance is required for all key personnel at award. The conducting of this level of back ground investigation is solely the responsibility of the Contractor.

The Key Personnel under this task order are the Project Manager, IT Security Specialist (senior), and Systems Engineer (for only two of the six requested).

7.0 TRAVEL AND ODC

7.1 Travel

Travel to any of the Customs locations may be required. The COTR/Task Monitor shall identify travel requirements on a case by case by basis. The COTR/Task Monitor must approve all travel requests. Any required 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 that 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. Travel in the not to exceed amount of $12,000 is anticipated for the first year of this effort. $18,000 (travel for option 1), $24,000 (travel for option 2), $30,000 (travel for option 3), and $36,000 (travel for option 4) is estimated for the option years.

7.2 Other Direct Cost

The Contractor shall acquire the COTR or his/her designee's approval on all ODCs prior to initiating any purchase and ODC expense. When submitting ODC requests, the Contractor should provide details such as which task area it supports and how it will support the task identified.

8.0 GOVERNMENT FURNISHED EQUIPMENT/MATERIALS/INFORMATION

Government material, equipment, and information are to be provided in conjunction with required performance under this SOW as needed. To include, but not limited to: Security monitoring and diagnostic devices as approved by the Architecture Review Board (ARB), telephones, personal computers, copy machines and office supplies.

As determined by mutual agreement, the Government shall provide additional property that may be required in the performance of the sub-tasks.

At the request of the Government, or at completion of the task order, the Contractor shall immediately return all Government provided property. This shall include all property or information that was provided by the Government for the Contractor to use to complete the assigned sub-tasks under this SOW.

All Government furnished information must be protected to the degree and extent required by local rules, regulations, and procedures. The 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.

9.0 OTHER INFORMATION PERTINENT TO THE REQUIREMENTS

The Government will furnish all software, data and equipment needed by the Contractor. An annual report of property in possession of the Contractor will be required of the Contractor under HSAR 3052.245-70 GOVERNMENT PROPERTY REPORTS (DEC 2003). Additionally, the Contractor shall be required to comply with HSAR 3052.237-71 INFORMATION TECHNOLOGY SYSTEMS ACCESS FOR CONTRACTORS (NOV 2004) (Deviation) and 3052.204-70 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (DEC 2003).

OIT will provide adequate working space for all Contractor employees, LAN access to those meeting the security requirements, standard desktop computers and peripherals (with appropriate software to perform the tasks in the SOW), and consumable supplies for personnel working directly on this contract.

9.1 Rights In Technical Data and Computer Software

CBP has unlimited rights against the Contractor, in the Computer Software and Technical data produced under this Task Order. CBP and the Contractor agree that CBP shall have the exclusive and absolute right, title and interest in and to all systems and software owned by CBP, or otherwise obtained, or developed at CBP expense, and furnished to the Contractor for use under this contract.

9.2 Place of Performance

Location: Work shall be performed primarily at the CBP National Data Center buildings or other CBP locations in the Washington, D.C. metropolitan area and within a 50-mile radius of the D.C. metro area.

Primary location is:
US CBP
National Data Center One (NDC1)
7681 Boston Boulevard
Springfield, VA 22153

Pursuant to Disaster Recovery Operation Center (DROC) processes and procedures, in the event of a test or actual catastrophic failure at the NDC sites, the CBP NDC would operate form a remote location outside of the D.C. metropolitan area. Some work shall be performed at the Commercial Recovery vendor's site. The work performed at the Commercial Recovery vendor's location will be scheduled and adhere to the Travel Section of this SOW.

9.3 Place of Delivery

All work products shall be provided to the personnel specified in Section 5.0 at the address indicated above no later than 4:30 PM local time on the delivery date specified.

9.4 Method of Delivery

Hand carry to OTM and COTR; or email (soft copy).

10. SECURITY

10.1 Personnel Security

10.1.1 Security Requirements

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

10.1.2 Personnel Security Background Data

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

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 CBP, and submit such information and documentation as may be required by the Government to have a BI performed.

The information must be correct and reviewed by the designated CBP 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 contract 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 Contracting Officer/COTR. This policy also applies to any personnel hired as replacements during the term of the contract order.

Upon award and when applicable, the CBP 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 contract personnel required to access SCI facilities and classified National Security information and applies to any and all personnel hired as replacements during the term of the contract order.

All background investigation forms must be accepted by CBP with verbal approval from a representative from CBP Office of Management Inspection and Integrity Assurance, Security Program Division (MIIA-SPD) before contract personnel can begin work under this order. MIAA-SPD estimates these procedures will take approximately ten (10) days from the time they receive the packet. Currently, completion of background

investigations is taking approximately six (6) months from initial acceptance of the package.

The Contractor shall notify the COTR and CBP Office of Information and Technology (OIT) Workforce Management Group (WMG), BI Coordinator 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 reassignments including those to another contract. The Contractor/Project Manager is responsible for the completion and timely submission to the COTR of the CF-242 for all departing contract personnel. The Contractor shall provide OIT/WMG/BI Coordinator the following information on behalf of their contract personnel to telephone number 703-921-6237 or fax the below information to 703-921-6780:

The Contractor shall notify the CBP OIT WMG of any change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, and terminations. The Contractor shall provide the following information to OIT WMG at Tel. (703) 921-6237 and FAX (703) 921-6780:

FULL NAME
SOCIAL SECURITY NUMBER
EFFECTIVE DATE
REASON FOR CHANGE

In accordance with Customs Directive No. 51715-006, "Separation Procedures for Contractor Employees (CF-242)", the Contractor is responsible for ensuring that contract employees separating from the agency complete the relevant portions of the CF-242. This requirement covers all Contact employees who depart while the contract is still active (including resignations, termination, etc) or upon final completion of contracts. Failure of a contract to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

10.1.3 Identification Badges

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

10.2 Additional Personnel Security Data

The Contractor shall ensure that their personnel use the following format signature on all official e-mails generated by CBP computers;

[Name]
[Position or Professional Title]
[Company Name]
Supporting the XXX Division/Office..
US Customs and Border Protection

[Phone]
[FAX]
[Other contract information as desired]

11.0 PERFORMANCE AND DELIVERY

Performance of Contractor employees shall be evaluated based on the amount of time to complete the work requested. An estimated time frame for completion of the service shall be stated in the Work Request. If the time frame needs to be extended, the Contractor should submit a justification to the COTR. If a Contractor employee frequently exceeds the estimated time frames without proper justification, the company agrees that the employee(s) shall be replaced at the COTR'S discretion. The Contractor shall agree to remove the person assigned within one day of official notification by CBP and provide a suitable replacement within a mutually agreed upon time frame. All new hires or substitutions of personnel are subject to CBP's Background Investigation requirement and the DoD Top Secret clearance requirement for key personnel.

11.1 Hours of Operations:

The SOC/CSIRC is a 24x7 operation, and work will be performed as shift work, enduring that personnel are onsite during core hours (7:00 a.m. to 6:00 p.m.), with adequate coverage during the off-shift hours. In the event of a classified spill, test Alert Level elevation or actual catastrophic failure, additional support personnel may be called in after their shift ends to provide continuous coverage during the event.

11.2.Holidays and Administrative Leave.

Bureau of Customs and Border Protection (CBP) personnel observe the following days as holidays:

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

Any other day designated by Federal statute, by Executive Order or by the President's proclamation.

When any such day falls on a Saturday the preceding Friday is observed. When any such day falls on a Sunday, 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, except as set forth in the contract.

The Contractor will not charge any holiday as a direct charge to the contract. In the event Contractor 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. However, this does not preclude reimbursement for authorized overtime work.

In the event CBP grants administrative leave to its Government employees, at the site, on-site Contractor personnel shall also be dismissed if the site is being closed, however, the Contractor shall continue to provide sufficient personnel to perform around-the-clock requirements of critical efforts already in progress or scheduled and shall be guided by the instructions issued by the Contracting Officer or her/his duly appointed representative. In each instance when the site 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 site(s) or taking appropriate leave consistent with its policies. The cost of salaries and wages to the Contractor for the period of any such site closure are a reimbursable item of direct cost under the contract for employees whose regular time is normally a direct charge if they continue to perform Task Order work; otherwise, costs incurred because of site closure are reimbursable as direct costs in accordance with the Contractor's established accounting policy.

The Contractor staff shall inform the COTR and OTM of all vacations and other time off. Due to the 24x7 nature of the CSIRC, it may not be possible for Contractor staff to observe the above stated holidays to ensure adequate coverage during Core Hours as stated above.

11.3 Overtime

Contractor personnel may not work more than 40 hours a week without prior approval from the Contracting Officer Technical Representative (COTR). Approved overtime hours shall be invoiced at the normal hourly rate.

12.0 NON-DISCLOSURE OF INFORMATION

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this SOW. The information shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of this order on an Official Use Only or need to know basis.

13.0 INVOICE REQUIREMENTS

The Contractor shall provide monthly costs reports to the COTR/OTM that shall include, at a minimum: man-hour cost data, travel data, percentage of work completed, and estimated costs remaining to complete the order.

To ensure timely processing of the Contractors invoices, the Contractor shall provide the COTR with copies of timesheets at the end of the timesheet period for each person with hours expended in support of the contract over the reporting period. The report format should be electronic mail and on backup storage media (compact disk).

Invoices shall contain the following information:

- Date invoice is issued;
- Contract number;
- Period of performance (start and expiration date);
- Funding Source (E.g. Base, CSI. COBRA, and ACS Life Support) which shall be identified to the Contractor upon award of the task order;
- For each funding source and task area listed, the contract labor categories and the names of the persons associated with the labor category;
- Contract labor category rate;
- Straight time labor hours by person (regular/extended time) [i.e., no overtime charges may be submitted; just straight time] over period of performance;
- Cumulative straight time labor hours by person (regular/extended time) for contract period of performance;
- Labor sub-totals for each funding category and task area;
- Travel and per diem charges by person for invoice period (with receipts for expenses incurred) and cumulative over the contract period;
- Other direct costs (ODCs) incurred during the period of performance with receipts or explanation of each item if no receipt or cumulative ODCs;

Invoices shall include Grand Totals for all funding sources, labor categories, travel and ODCs for the contract. The next pages of the report shall contain the following fields:

Period of performance expiration date, Hours-the number of hours billed against the contract for that month; Cost – this is the amount billed against the contract for that month; Allocated - this is the award amount of the contract (i.e., this is the amount the Government obligated to the contract); Cumulative - this is the amount billed against the contract since the beginning of the contract; PCT - This the percentage billed to date, remaining – This is the amount remaining on the task assuming that month's invoice is approved to date.
The invoice shall contain the following statement signed and dated by an authorized company representative: "This is to certify that the services set forth herein were performed during the period stated."

13.1 Invoice Submission

The vendor shall invoice the Government monthly for services performed under the contract. Invoices shall be for services, travel and ODCs incurred against the contract during the previous month's period of performance. The period of performance shall begin on the first of the month and end on the last day of that month. Invoices shall be received by the tenth day of each month and include billable items for the previous month's period of performance. In addition to sending the invoice to Indianapolis, a copy shall be submitted to the COTR at the following address:

US Customs and Border Protection
7681 Boston Boulevard, NDC1 Rm. 2014
Springfield, Virginia 22153
Attn: (b) (6) [redacted]

13.2 Invoice Modification

The Contractor shall endeavor to ensure that all employee timesheet submissions and all travel receipts are accurate and valid, and as such, the invoices submitted to the Government should not require future changes. In the event that an error is made, the change shall be recorded and invoiced within ninety (90) days of the last day of the month in which the labor or travel was performed or the ODC was purchased. In addition, any such adjustment shall contain detailed documentation explaining the error and the time period during which it occurred. No changes shall be accepted after ninety (90) days of the end of the period of performance.

At the COTR's discretion, the format of the invoice may be changed. The COTR shall notify the Contractor of the change in format at least 60 days prior to requiring its use by the Contractor.

14.0 CONTRACTING OFFICER TECHNICAL REPRESENTATIVE

Contract deliverables shall be provided to the following specific points of contact:

CBP, COTR
(b) (6) [redacted]
US Customs and Border Protection
7681 Boston Boulevard, NDC1 Rm. 2014
Springfield, Virginia 22153
(b) (6) [redacted] @dhs.gov
(703) (b) (6) [redacted]

APPENDIX A: SOC SERVICE LEVEL OBJECTIVES

Desired Outcomes	Required Services	SLO Performance Objective (completeness, cost, reliability, accuracy, timeliness, quality)	Acceptable Quality Level (AQL)	Monitoring Method (Quality Assurance Surveillance Plan/QASP)	Target AQL
Device Monitoring and Analysis	Monitor the network for security policy compliance	The DHS SOC shall provide the capability to receive and monitor security event data from security devices as defined in SOW 24 hours a day 7 days a week 365 days a year. Ensure constant, uninterrupted monitoring of the Network.	SOC operation availability of 90% of 24x7	Network connectivity to the systems in the SOC (not dependent on outages within the subscribers LAN), System uptime, Application uptime, Device audit trail and system log review.	99.999 SOC availability
Customer Service	Time to answer trouble report	60 seconds, not more than 4 rings to maintain efficiency of operations (non-automated response)	90% of all call answered by an analyst within 4 rings (60 seconds).	Automated telephone log report provided to management by Newington Phones	99% of all calls answered by an analyst within 4 rings (60 seconds)
Customer Service	Time to respond to trouble report	Open a Remedy ticket, respond via email or log incident case in SOC On-line within15 minutes of receipt	90% of all trouble calls logged	Remedy ticket reports provided to management	99% of all trouble call logged
Security Event Detection	Security Event Detection of suspicious user or anomalous network behavior or traffic patterns against normal expected or baseline network activity, posing a threat to the availability of a critical system or indicative of a violation of Federal law or DHS Policy.	Detection must occur within 4 hours of security event initiation. Initial event analysis or case to be assigned to an analyst for further review and validation.	Baseline: Detection of 90% of all network events indicative of anomalous or malicious or violation activity against critical systems.	Periodic sampling of analyst cases, and routine reports using available security technologies, to include Host Intrusion Detection (HIDs), Network Intrusion Detection (NIDs), Anti-virus, and SIM database tools.	**Incentive:** Detection of 99.9% of all anomalous network events against critical systems,
Security Event Notification	Provide timely and accurate analysis of security detected security events.	Contractor must present evidence that the Contractor SIM technology discovered the event and that Security Operations Center Personnel recognized it as such and initiated analysis within 4 hours of event detection. Acceptable evidence includes security event case logs, Incident reports to DHS CSIRC, Security Event Notifications, and tickets opened for LAN remediation.	**Baseline:** Analysis of 90% of SIM cases initiated within 4 hours. Closure of reports based on priority and classification.	Periodic sampling of analysts cases to determine time to closure, 90% of all cases closed with 1 week. SIM-Generated cases with a high rating will be evaluated separately.	**Incentive:** Analysis of 90% of high SIM Tickets initiated and closed within 24 hours.
Incident Management	Security Event Response Restoration of service Termination of activity and/or	Upon reporting of a bona-fide (validated) security event, action is taken to determine the scope and minimize the effects of the event, restore any lost capability and prevent	Notification to WAN Network support team, LAN system admin for containment and eradication:	The Security Incident Tracking Systems keeps a timestamp of this activity and may be queried at any time at view this metric.	Incentive: Appropriate reaction and containment of 99.9% of Incidents,

Desired Outcomes	Required Services	SLO Performance Objective (completeness, cost, reliability, accuracy, timeliness, quality)	Acceptable Quality Level (AQL)	Monitoring Method (Quality Assurance Surveillance Plan/QASP)	Target AQL
	removal of malicious code (Virus, Trojan Horse, Worm, Mobile Code, Blended Attack) Terminating the activity. Technically and Logically removed from the network. Mean time to Terminating the activity will only be measured;	similar events from happening in the future. Actions should be consistent with the Incident Response Plan, however; only the end state is measured. The desired end state and time frame will vary depending on the type of security event. Critical (see escalation) Moderate Low Informational	Low to Moderate Containment (at firewall or Policy Enforcement Points) within: 24 hours after receiving direction from the governing authority (CSIRC/CCB). Logical Removal: 1 week after receiving direction from the governing authority (CSIRC/CCB).		
Incident Escalation	Incident Escalation for Security Event Response	The DHS SOC shall provide Security Event Notification to the DHS authorized contacts for all verified CRITICAL security events as defined	Via email within 4 hours of confirmed event. Via telephone within 4 hours of confirmed event.	The Security Incident Tracking Systems keeps a timestamp of this activity and may be queried at any time at view this metric.	
SOC system availability	The DHS SOC shall provide the capability to receive and monitor security event data from SOC security devices 24 hours a day 7 days a week 365 days a year.	Not to exceed 4 hours per month during "quiet" hours at non-critical sites. Key sites should not require scheduled downtime as backup facilities should be invoked during maintenance.	90% availability	Network connectivity to the systems in the SOC (not dependent on outages within the subscribers LAN), System uptime, Application uptime, evidence in system logs and audit trails	99.999%
SOC system maintenance	DHS Notification Criteria for Scheduled Maintenance	Contractor must update IDS systems; download signature updates and rulesets as released by vendors or advisories within 5 business days. Contractor may provide 14 days advance notice for testing of rules maintenance operations. Maintain efficiency of operations and Steward oversight	90% availability	Configuration of the systems in the SOC (dependent on vendor support agreement) release and change management. System configuration and validation evidenced by self-assessment scans.	99.999%
Audit/Vulnerability Assessment	Protection of data and systems and prevention of further attacks	Review scan data and OS specific collect script output and identify services, permissions, and settings that are not in compliance with Unix and windows security	Provide system owner a VA summary report. Alert System Owner, ISSO, and/or LAN Management of	Provide management summary report of automated vulnerability assessment scans conducted in accordance with a master schedule. Provide management	100% high vulnerabilities reduction or documented exemption

FAR 52.204-2

Security Requirements (Aug 1996)

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

(b) The Contractor shall comply with—

(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DoD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

(End of clause)

Section H- Special Contract Requirements

H.1 Cooperation with Other Contractors

The Contractor shall fully cooperate with the other prime contractors and with Government employees and shall carefully adapt scheduling and performing the work under this contract to accommodate the work being performed under the other contract, heeding any direction that may be provided by the Contracting Officer. The Contractor shall not commit or permit any act that will interfere with the performance of work by any other contractor or by Government employees.

(END OF CLAUSE)

Desired Outcomes	Required Services	SLO Performance Objective (completeness, cost, reliability, accuracy, timeliness, quality)	Acceptable Quality Level (AQL)	Monitoring Method (Quality Assurance Surveillance Plan/QASP)	Target AQL
		standards. Review rule base and identify rules that permit risky protocols. Review OS and devices that are not incompliance with standards.	any high /critical vulnerability on backbone network within 4 hours of identification, AQL is 85% high vulnerabilities reduction or documented exemption	compliance report and coordinate remediation. Track differential and progress between scans	
Vulnerability Assessment Penetration Testing	"Ethical Hacking" to discover and mitigate system vulnerabilities	Coordinate with system owner under a formal rules of engagement authorization for system penetration testing	Schedule and conduct pen testing IAW with established ROE within 14 days of request.	Provide Penetration tests summary of findings, recommendations and alert system owner to high vulnerabilities.	Mitigation of 100% of system high vulnerabilities
Vulnerability Management	Monitor an d release notification of advisories and bulletins	Hardware Components and critical designated components, to include boundary components, servers, workstations, routers, and switches. Designated components as described in the Technical Reference Manual, respective SSPs., and approved Change Request (CRs)	**Baseline:** 95% of ISVM are released within 24 hours of receipt from approved sources. Components are complaint upon evaluation.	The Security Incident Tracking Systems keeps a timestamp of this activity and may be queried at any time at view this metric.	Incentive: 99% of ISVM released with 4 hours and Components acknowledge receipt of the ISVM. and are complaint upon evaluation
Digital Forensics	Incident Investigation; Collection of Evidence	Bets practices data collection, examination, analysis and reporting. Maintaining chain of custody and storing evidence securely.	Integrity of log files in a forensically sound manner.	Management inspection of Record keeping logs including timekeeping, case management, case incident reports	Admissibility of collected evidence into legal proceedings
Web Based reports	Online reporting capabilities: OneNet view of user authentication activity and trouble-ticket status visibility	Support FISMA Incident Reporting and tracking, Customer portal for reporting and viewing information, blog, scan request maintain uptime, and efficient operations of the SOC.	Web portal availability of 99.2% of 24x7 that includes the duration of non-scheduled maintenance but excepts scheduled maintenance	Provide Management account on web portal to review reports and query performance metrics.	No deviation from established timeline.
Reporting	Status and performance reporting	Contractor to deliver a monthly status and performance report	Provide quarterly FISMA reports within established timelines.	Management inspection of written contractor monthly report and collection of FISMA data	Report publish on time- no deviation