

# ORDER SUPPLIES OR SERVICES

PAGE OF PAGES

1 2

**IMPORTANT: Mark all packages and papers with contract and/or order numbers.**

1. DATE OF ORDER 03/01/2010		2. CONTRACT NO. (if any) HSHQDC-06-D-0026		6. SHIP TO:	
3. ORDER NO. HSBP1010J00159		4. REQUISITION/REFERENCE NO. 0020047949		a. NAME OF CONSIGNEE See Attached Delivery Schedule	
5. ISSUING OFFICE (Address correspondence to) DHS - Customs & Border Protection Department of Homeland Security 1300 Pennsylvania Ave., NW NP 1310 Washington DC 20229				b. STREET ADDRESS	
c. CITY		d. STATE	e. ZIP CODE		
7. TO:				f. SHIP VIA	
a. NAME OF CONTRACTOR SCIENCE APPLICATIONS INTL CORP				8. TYPE OF ORDER	
b. COMPANY NAME				<input type="checkbox"/> a. PURCHASE - Reference Your _____ Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	
c. STREET ADDRESS 8301 GREENSBORO DR STE 290				<input checked="" type="checkbox"/> b. DELIVERY - Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.	
d. CITY MCLEAN		e. STATE VA	f. ZIP CODE 22102-3608		
9. ACCOUNTING AND APPROPRIATION DATA  See Attached Accounting and Appropriations Data  CONTRACTOR TIN: (b)(3); (b)(4)				10. REQUISITIONING OFFICE EDME	
12. F.O.B. POINT Other				11. BUSINESS CLASSIFICATION (Check appropriate box(es))	
13. PLACE OF				<input type="checkbox"/> a. SMALL <input checked="" type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. EMERGING SMALL BUSINESS <input type="checkbox"/> g. SERVICE-DISABLED VETERAN-OWNED	
a. INSPECTION		b. ACCEPTANCE		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B POINT ON OR BEFORE (Date) 03/01/2010
				16. DISCOUNT TERMS Net 30	

**17. SCHEDULE (See reverse for Rejections)**

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	Acpt
10	Enterprise Security Support	1.000	AU	(b)	(4)	
20	ODC/Travel	1.000	AU	(b)	(4)	
30	Enterprise Security Support - ACE	1.000	AU	(b)	(4)	
40	Enterprise Security Support - CSI	1.000	AU	(b)	(4)	

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		TOT. (Cont. pages)
21. MAIL INVOICE TO:						
SEE BILLING INSTRUCTIONS REVERSE	a. NAME DHS - Customs & Border Protection		National Finance Center		\$0.00	
	b. STREET ADDRESS (or P.O. Box) PO Box 68908				\$6,194,621.00	
	c. CITY Indianapolis		d. STATE IN	e. ZIP CODE 46268		
22. UNITED STATES BY (Signature) (b) (6)		23. NAME (Typed) STEPHON DOSWELL		(REV.)		
		TITLE: CONTRACTING/ORDERING OFFICER				

AUTHORIZED FOR LOCAL REPRODUCTION  
Previous edition not usable

OPTIONAL FORM 347 (4/2006)  
Prescribed by GSA/FAR 48 CFR 53.213 (f)

DATE OF ORDER 03/01/2010	CONTRACT NO. (if any) HSHQDC-06-D-0026	ORDER NO. HSBP1010J00159	PAGE OF PAGES 2 2
-----------------------------	---	-----------------------------	----------------------

**Federal Tax Exempt ID: 72-0408780**

**Emailing Invoices to CBP.** As an alternative to mailing invoices to the National Finance Center as shown on page one of this award you may email invoices to: [cbpinvoices@dhs.gov](mailto:cbpinvoices@dhs.gov).

**NOTES:**

This labor hour type task order, HSBP1010J00159 has been issued to replace modification HSBP1007J14516P00006.

This task order has been issued due to a conversion error between SAP and PPS. This task order number, HSBP1010J00159, will now be used in lieu of HSBP1007J14516. However, the terms and conditions of award HSBP1007J14516 remain in full effect.

Modification HSBP1007J14516P00006, dated 12/24/2009, is hereby voided. This task order, HSBP1010J00159, will be used as a replacement for HSBP1007J14516P00006.

Option Period 3 remains exercised for \$6,194,621.00. As a result of this task order, the total amount of this order remains as \$29,605,226.32.

The Period of Performance for Option Period 3 remains 01/01/2010 through 12/31/2010.

All terms and conditions of HSBP1007J14516 remain in full effect.

**ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA  
FOR  
DELIVERY ORDER: HSBP1010J00159**

**I.1 SCHEDULE OF SUPPLIES/SERVICES**

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	Enterprise Security Support	1.000	AU	<b>(b) (4)</b>	<b>(4)</b>
20	ODC/Travel	1.000	AU		
30	Enterprise Security Support - ACE	1.000	AU		
40	Enterprise Security Support - CSI	1.000	AU		

**Total Funded Value of Award:**

**\$6,194,621.00**

**I.2 ACCOUNTING and APPROPRIATION DATA**

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2525USCSGLCS0923030000Z64J10400HQ01 IR2332525	<b>(b) (4)</b>
20	6100.2525USCSGLCS0923030000Z64J10400HQ01 IR2332525	
30	6100.2525USCSGLCS0923030000Z64J10165HQ01 IR2332525	
40	6100.2525USCSGLCS0923030000Z64J10400AP03 171502525	

**I.3 DELIVERY SCHEDULE**

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
SCIENCE APPLICATIONS INTL CORP 8301 GREENSBORO DR MCLEAN, VA 22102-3608	10	1.000	10/01/2009
	20	1.000	10/01/2009
	30	1.000	10/01/2009
	40	1.000	10/01/2009

**Statement of Work  
Enterprise Security Service (ESS) Support  
for  
Bureau of Customs and Border Protection (CBP)  
Office of Information and Technology (OIT)  
Program Integration Division (PID), Security and Technology Policy Branch (STP)**

PR 2004-7949  
POP (01/01/10 thru 12/31/10)

## **1.0 Background**

The Bureau of Customs and Border Protection (CBP), Office of Information and Technology (OIT), Program Integration Division (PID), Security and Technology Policy Branch (STP), is responsible for providing enterprise security service (ESS) support to CBP and the Department of Homeland Security (DHS).

This support includes, but is not limited to, the following:

- Certification and Accreditation (C&A) support for systems and applications.
- Risk assessments of CBP and select Department of Homeland Security (DHS) sites, as needed.
- Promoting DHS Sensitive System Policy Directives 4300B.
- Identifying and analyzing security risks and mitigation solutions.
- Governing and enforcing security policies.
- Communication Security (COMSEC).
- Developing CBP information system security policies, standards and procedures for both CLASSIFIED and Sensitive but Unclassified (SBU) systems.
- Liaison activities within CBP, the Department of Homeland Security, other government agencies including law enforcement agencies, the international trade community and private firms as they relate to security compliance issues, security programs, policies, issues and products.
- Security architecture development and oversight.
- Training support to the Office of Training and Development (OTD) as Subject Matter Experts.

DHS Chief Information Officer (CIO) has mandated 100 percent certification and accreditation of all DHS Major Applications (MA) and General Support Systems (GSS). The DHS Chief Information Security Officer (CISO) tracks each DHS component's C&A progress. In order to standardize the C&A effort throughout DHS, DHS has mandated the use of two software products: Risk Management System (RMS) and Trusted Agent FISMA (TAF). Only artifacts created using DHS mandated software shall be accepted for credit. STP works on a program-by-program basis, to assure all the systems security documentation and information is complete and ready for the CBP C&A process.

## **2.0 Scope of Work**

The scope of this Statement of Work (SOW) encompasses contractor development of a program to provide enterprise-wide systems security support to STP, including, but not limited to; C&A, risk assessments and mitigation strategies, CLASSIFIED Systems, COMSEC, security policy and procedures, security architecture and Security Test and Evaluation.

The contractor shall be accountable for maintaining and reporting accurate and current technical, administrative and financial status of the IT security program, and other related activities. The contractor shall submit this information in periodic status reports described elsewhere in this document.

The contractor shall provide technical and administrative support personnel who are well qualified and are willing to become familiar with the policy and regulations of CBP.

## **2.1 Personnel Security**

All personnel employed by the contractor or responsible to the contractor for the performance of work hereunder shall either currently possess or be able to favorably pass a full-field background investigation (BI) based on information from the prior seven years of employment. Personnel supporting CLASSIFIED and COMSEC tasks shall also possess or shall be able to obtain a Top Secret clearance with Sensitive Compartmented Information (SCI).

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 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.

In addition to a personnel full-field BI, the contractor shall submit a DD 254 for those employees that require additional background information needed to authorize access to National Security Information. New hires or substitutions of personnel are subject to the CBP BI clearance requirements.

All BI forms must be delivered to the CBP, Office of Information & Technology (OIT), Personnel Security Branch, Workforce Management Group (WMG) before the employee can work on this contract. After WMG reviews and accepts the BI package,

they forward it to Internal Affairs (IA) for determination of suitability. Until IA initiates a full-field BI and the contractor employee passes the TECS/NCIC/Credit Check, he/she will not be issued a badge, must be escorted at all times while on CBP premises, and will not have access to any CBP systems or sensitive information. If the contractor employee passes the initial TECS/NCIC/Credit checks, he/she is granted a "LIMITED" BI, which enables the employee to have a badge and restricted access to sensitive information. With the "LIMITED" he/she no longer requires an escort.

If the contractor employee fails the TECS/NCIC/Credit checks, his/her BI is put into a "DELAY" status and he/she will not be granted any additional access until the full-field BI is completed. If the contractor employee is put into this "DELAY" status, he/she will not be allowed to work on or bill to this contract until the full-field BI has been successfully adjudicated.

WMG estimates that the TECS/NCIC/Credit check procedures may take one (1) month or longer from the time the packet is received. Completion of the full-field BI may take at least another 90 days.

The contractor shall notify the COTR and Contracting Officer via phone, FAX, or electronic transmission, no later than one workday after any personnel changes occur. Written confirmation or phone notification is required. This includes, but is not limited to, resignations, terminations, and reassignments including those to another contract.

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. (b) (7)(E) and FAX (b) (7)(E)

Full Name  
Social Security Number  
Effective Date  
Reason for Change

### 3.0 Tasks

#### 3.1 Task Area 1. Certification and Accreditation

The contractor shall provide technical security expertise in planning, preparing and executing certification and accreditation support for Customs & Border Protection. In support of this task, the contractor shall ensure that CBP information systems and technology are secure and meet all applicable security requirements. In attaining this goal, the contractor shall support the Security & Technology Branch with the review and support of certification and accreditation documentation, participation in technical meetings, on-site observations, efficient use of automated accreditation tools and preparation of technical papers.

Each member of the C&A team shall serve as the Certification Agent (CA) and/or the Information Systems Security Officer (ISSO) for several systems, which include CLASSIFIED and SBU major applications and general support systems. However, the team member shall not serve as both the CA and the ISSO for the same Information system. Furthermore, in order to eliminate any conflict of interest, Government Leads shall serve as the Certifying Agents for any systems for which an STP contractor serves as the ISSO. All artifacts in support of the C&A must meet Federal, DHS and CBP requirements.

### **3.1.1 Certification Agent (CA) Support for Certification and Accreditation (C&A)**

The contractor shall provide personnel to perform CA duties in support of the C&A process at CBP. The CA assigned to an Information Technology (IT) system shall serve as the subject matter expert for security. The CA shall be a point of contact in STP to provide security solutions and interpretations of security policies as they relate to specific architectures and projects. The CA shall establish rapport and develop a relationship with the project development team(s). A CA shall typically serve in that role for more than one system. The CA shall perform duties including but not limited to:

- Supporting audits.
- Monitoring timeliness of accomplishment of required actions and documents pertaining to the C&A of the system throughout its lifecycle.
- Ensuring that an Information Systems (IS) security analysis is conducted to determine appropriate security requirements during the design stage of an application.
- Ensuring that the IS design meets a specified set of security requirements.
- Assisting developers in ensuring IS security requirements for all applications comply with all laws and regulations and are appropriate and sufficient.
- Creating the Security Assessment Reports for the C&A process.
- Ensuring IS security plans and other C&A documents are developed for all applications following DHS and CBP mandated procedures and tasks, such as using RMS.
- Providing written justification, when appropriate, to the Chief, STP Branch for approval by the Assistant Commissioner, Office of Information and Technology (OIT) to obtain a written waiver of policy for mandated security features.
- Coordinating with the assigned Information Systems Security Officer (ISSO) on deployment of new systems and modifications of legacy systems.

- Ensuring that the system/application meets the minimum DHS/CBP certification & accreditation standards before a recommendation is made to the CBP ISSM. Once certification recommendation is accepted by CBP ISSM, the contractor shall upload all relevant C&A artifacts onto the DHS-approved repositories (e.g., Trusted Agent FISMA (TAF)).
- Possessing an understanding of how to determine when security discrepancies exist through knowledge of Federal/DHS laws and security policies, as well as current technologies and architectures. These include understanding the comprehension of CBP's mission, tasks and deliverables for process improvement, and overall risk management.
- Identifying improvement for the accreditation process where practical to lessen: processing time; the amount of paperwork; and resources required, to include benchmarking and other process improvement activities.

### **3.1.2 Information Systems Security Officer (ISSO)**

The contractor shall provide personnel to perform ISSO duties in support of the C&A process at CBP. The ISSO shall be a point of contact in STP to provide security solutions and interpretations of security policies as they relate to specific architectures and information systems (IS's). The ISSO shall establish rapport and develop a relationship with the system development team(s) to become a recognized and integral member of the team. An ISSO shall typically serve in that role for more than one project. The ISSO shall perform duties including but not limited to:

- Participate in appropriate actions to certify and accredit each IS.
- Notify the ISSM when an assigned system requires accreditation or reaccreditation.
- Assist in the certification and accreditation of each system.
- Provide policy and technical advice to systems designers, implementers and operators.
- Conduct risk assessments and prepare an appropriate summary of findings for inclusion within the accreditation documentation.
- Conduct self-assessments of the CBP major applications and general support systems, which shall include vulnerabilities identified at contractor/consultant facilities.
- Recommend corrective actions for deficiencies found during system self-assessments (NIST 800-26) reviews and or during any review or monitoring period for the system/application.
- Ensure timely Plan of Actions & Milestones (POA&Ms) are updated and uploaded in the Trusted Agent FISMA tool. (i.e., by March 10, June 10, September 15, and December 10 annually).

- Draft, review and endorse all information systems security plans and other C&A artifacts, not including the Security Assessment Report (SAR). These artifacts include but are not limited to the following:
  - Privacy Threshold Determination
  - Privacy Impact Assessment (PIA)
  - E-Authentication Determination
  - Controls Testing (Security Test and Evaluation (ST&E)) Plan
  - ST&E Plan Test Results
  - System Security Authorization Agreement (SSAA) (for CLASSIFIED systems)
  - Authorization to Operate (ATO) Authorization Letter
  - Self Assessment (National Institute of Standards and Technology Special Publication (NIST SP 800-26) *NIST DRAFT Special Publication 800-26, Revision 1: Guide for Information Security Program Assessments and System Reporting Form*)
  - *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199) Assessment
  - Risk Assessment
  - System Security Plan
  - Contingency Plan
  - Contingency Plan Test Results
  - Security Test & Evaluation
  - Security Assessment Report
  - Plans of Actions & Milestones (POA&Ms)
  - Authority to Operate Letter
  
- At the request of CSIRC, assist in the investigation of security violations and incidents.
- Be knowledgeable on current Federal, National, DHS and CBP standards, policies, requirements and procedures.
- Complete/update a NIST SP 800-26 or NIST SP 800-53 review for each major application or general support system on a yearly basis. Review and update System Security Plan annually and when significant security changes occur

### **3.2 Task Area 2 - Communications Security (COMSEC)**

COMSEC is the system of security measures used to protect classified information or material utilizing cryptographic keying material and equipment. COMSEC measures are taken to deny unauthorized personnel information derived from telecommunications of the U.S. Government concerning national security and to ensure the authenticity of such telecommunications. COMSEC includes cryptography, transmissions security and physical security of communications security material and information.

Currently CBP utilizes the services DHS COMSEC Office of Record (COR). In the future CBP may opt to recreate its own centralized COMSEC COR.

### **3.2.1 COMSEC Custodian**

The contractor shall serve as COMSEC Custodians for accounts specified by the Chief, STP Branch. The contractor shall perform COMSEC Custodian duties including but not limited to:

- Receipt, custody, issuance, safeguarding, accounting for and when necessary, destruction of COMSEC material for offices and/or operating units under their areas of responsibility.
- Maintaining up-to-date records of COMSEC inventory and submitting required accounting reports.
- Administering initial briefing and debriefing to individual users.
- Maintain copies of all briefings and debriefings.
- Undergo required COMSEC training within six months of appointment and update training yearly.
- Programming and local distribution of COMSEC devices such as the Secure Telephone Equipment (STE) and QSEC 2700, a secure cell phone.
- Receipt, loading and management of COMSEC keying material using devices such as the Electronic Key Management System (EKMS), Data Transfer Device (DTD), Simple Key Loader (SKL) and Secure DTD-2000 System (SDS).

### **3.2.2 COMSEC COR Duties**

The contractor shall provide COMSEC COR services related to the distribution, governance and maintenance of keying material, secure phones and other COMSEC equipment. The contractor shall perform duties including but not limited to:

- Manage and perform centralized COMSEC accounting functions for CBP.
- Provide keying material for CBP with the use of EKMS.
- Perform NSA required audits of each COMSEC account in CBP every 18 months to ensure compliance with NSA and DHS policies.
- Provide COMSEC Custodian and COMSEC equipment training.
- Provide a Help Desk for technical and administrative questions.
- Evaluate new COMSEC equipment and fax machines for use by CBP.
- Represent CBP on Intelligence Community and National Security Agency Policy Working Groups and Committees.
- Provide Controlling Authority function for all CBP COMSEC keying material.
- Appoint new COMSEC Custodians.
- Set up new COMSEC accounts.
- Support COMSEC users on the set up of new secure communications circuits to meet mission needs.
- Provide assistance visits to CBP COMSEC accounts.
- Manage centralized maintenance contracts for COMSEC equipment.

- Maintain a pool of COMSEC equipment, to provide immediate replacement of operational equipment for use in establishing emergency circuits and to replace equipment in need of repair.
- Maintain visibility of all COMSEC assets in CBP to allow cross leveling of equipment or to direct a transfer of excess equipment to meet operational requirements.
- Coordinate and manage centralized Memorandum of Agreement (MOA) and funding for Defense Courier Services (DCS) support.
- Provide technical support to CBP to facilitate interoperability of purchases of COMSEC equipment.
- Provide a central Point of Contact (POC) for secure phone service with vendors such as T-Mobile, Verizon and ATT.
- Provide centralized support service for Satellite phone equipment and service.
- Advocate CBP issues with NSA and the Intelligence Community, to ensure the CBP perspective is heard in operational and policy forums.
- Complete documents and updates to databases as required by DHS 4300B, National Security Systems Handbook. The documentation includes but is not limited to: COMSEC account information, COMSEC Custodian training documentation, COMSEC Facilities documentation, COMSEC Material Accounting, and, COMSEC Incident Reports.

### **3.3 Task Area 3 - System Architecture**

#### **3.3.1 ESS System Architecture**

STP has an Enterprise Systems Security Catalog (ESSC) application. The contractor shall assist CBP Security and Technology Policy Branch (STP) in the maintenance of the Enterprise Security System (ESS) Architecture through updates to the ESSC, which include but are not limited to design improvements and updates to the contents of the catalog. The contractor shall identify requirements, establish an Enterprise Information System Architecture (EISA) compliant security architecture template and develop a compliant integrated security architecture and technical reference model (TRM).

The integrated security architecture (voice, video and data) shall be developed based on a top-down approach which defines the necessary services to ensure the confidentiality, integrity, availability, access control, accountability and non-repudiation of CBP systems, networks, applications and infrastructure. The architecture shall consist of three main components: functional architecture (security operations concept), security services architecture and a technical reference model. The architecture shall be based on policy, risk and best-practice-driven requirements. The contractor shall ensure that compliance with DHS and other government agencies (OGA) directives is maintained while ensuring the overall interoperability of the all the components of the Enterprise Security System.

Subcomponents of the architecture may include key management, public key infrastructure, intrusion detection and security management infrastructure that shall ensure the effective management of the security components and provide visibility into the infrastructure of the CBP security posture at any given instance.

The technical reference model (TRM) developed as part of the architectural effort shall form the basis for selection of interoperable products, algorithms, services and security applications programming interfaces.

### **3.3.2 ESS System Design Support**

The contractor shall provide support to assess current and emerging technologies for applicability to and compatibility with the EISA and ESS architecture and design. This includes but is not limited to security reviews in support of the Enterprise Architecture Technical Insertion (TI) process.

### **3.4 Task Area 4 - Technology Policy Administration (includes Section 508)**

STP reviews and establishes all IT policy for the CBP Office of Information and Technology (OIT). These policies include the management and security protection of both classified and sensitive information systems and data. STP also assists in the proper implementation of Section 508 Law with respect to electronic and information technology.

#### **3.4.1 Technology Policy**

The contractor shall perform the following duties to include, but not limited to:

- Draft, review, update and coordinate CBP reviews and approval of OIT policies to include the CBP Information Security Policies and Procedures Handbook, User Guide and Rules of Behavior.
- Develop the capability to assess and update existing policies and procedures, to ensure they correctly address any new threats to technology, new vulnerabilities and any changes to business operations. The Policy update process shall include receiving and evaluating policy comments from CBP users and organizations.
- Evaluate the effectiveness and adequacy of existing CBP policy as part of the continued monitoring and assessment of the CBP security posture.
- Develop and prepare a response/recommended CBP position to security policy directives and guidance issued by organizations such as Department of Homeland Security, the Office of Management and Budget (OMB), Public Law and the National Institute of Standards and Technology (NIST).
- Assist in developing process improvement procedures.
- Request, collect and prepare information for the STP Monthly Report.

- Monitor and control database for tracking Interconnection Security Agreements.

### **3.4.2 Section 508**

In 1998, Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily. Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities and to encourage development of technologies that will help achieve these goals. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508 (29 U.S.C. 794d), agencies must give disabled employees and members of the public access to information that is comparable to the access available to others.

The contractor shall perform the following duties to include but not limited to:

- Assist the CBP Section 508 Coordinator in proper implementation of Section 508 Law.
- Ensure CBP policies adhere to Section 508 Law.
- Provide expert advice and assistance to CBP Program Offices to ensure major applications and general support systems adhere to Section 508 Law.
- Perform Section 508 Training to CBP employees.

### **3.5 Task Area 5 - Security Risk Assessment**

STP is tasked to conduct Security Risk Assessments (SRAs) of its Local Area Network (LAN) systems throughout the United States and the world, as needed. The number of trips scheduled to perform the SRAs should be considerably less since sites in close proximity are assessed in a single trip. In order to assess the overarching security posture of CBP field sites, a sample of CBP field locations are visited in order to identify the likelihood of threats occurring, the controls in place to prevent or minimize exploitation of the vulnerabilities found, and the severity of the impact on the CBP mission of a threat exploiting identified vulnerabilities. The SRA and Report are based on guidance from NIST SP 800-30, NIST SP 800-26 and NIST SP 800-53. The contractor shall perform risk assessments to support such CBP functional areas that require connection to the CBP network.

The contractor shall review a sampling of the following types of CBP field LAN sites:

- Office of Field Operations (OFO) port offices, cargo inspection areas, field offices, airports, and pre-clearance sites;
- OIT field laboratories;
- OIT LANs in the Washington, DC metropolitan area;
- Office of Air and Marine branch offices;

- Office of Border Patrol branch locations;
- Office of International Affairs Container Security Initiative (CSI) sites; and
- Any other DHS component sites as they migrate to the CBP network.

The contractor shall perform duties including but not limited to:

- Support audits by providing information dealing with LAN risk assessments and related methodology.
- Schedule risk assessments based on importance of the site's mission, type of site (e.g., CSI, Pre-Clearance, Border Patrol branch office, ICE, airport, cargo inspection areas, port offices, laboratories, cargo inspection areas, field offices, Air and Marine branch offices, field offices), geographic area of site location (i.e., sampling of sites from each region and system, and size of site (i.e., number of terminals supported by the LAN at the site).
- Plan and coordinate site visit with the field office (i.e., notify them of the planned visit, collect and review all available information and data available at the site (e.g. LAN Continuity of Operations Plan, Physical Security Assessment Report, Floor Plan, Organization Plan, Mission Statement and artifacts from any prior Security Risk Assessment).
- Coordinate network vulnerability scans with the Computer Security Incident Response Center (CSIRC) and review the scans for high-risk network vulnerabilities.
- Perform a physical inspection of the site and minimally interview the LAN administrator, site management, and system users using documented interview questions.
- For each LAN site SRA characterize the organization and mission, identify supporting assets, identify threats, identify existing security controls and vulnerabilities, and map to controls and vulnerabilities to those recommended by NIST SP 800-53 guidance.
- From the data collected from the pre-assessment phase of the SRA, physical inspections, and interviews; determine likelihood of identified threat occurrences, severity of impact on the CBP mission if a vulnerability is exploited, and associated risk ratings. Develop recommendations regarding mitigation strategies for all identified vulnerabilities.
- Within one month of the SRA at the CBP LAN sites, deliver the Security Risk Assessment Report documenting a description of the mission performed at the locations visited, pertinent physical characteristics of the site and its security posture including supporting assets, threats, vulnerabilities, security controls identified.

- Populate a Plan of Action and Milestones (POA&M) table with the significant vulnerabilities identified by each SRA. Capture this information in the SRA database used to track the progress of the remediation.
- Plan and organize monthly POA&M meetings with the organizations that manage each type of site both from a functional and IT perspective.
- At these POA&M meetings, determine and plan the risk mitigation strategies and/or levels of acceptable risk, establish milestones and estimate the time to mitigation/resolution of vulnerabilities.
- Continually track and update milestones until resolution of the vulnerabilities. Include the information in the SRA database and in TAF, the DHS tool. Update TAF on a monthly basis with any changes in status.

### **3.6 Task Area 6 - Security Test and Evaluation:**

The contractor shall perform Security Testing and Evaluation of a select number of the CBP General Support Systems and applications in support of their Certification and Accreditation and continued improvements to the CBP security posture.

- Personnel must have technical expertise in performing security evaluations of all CBP major applications, Operating Systems and network Internet Operating System (IOS). This includes but is not limited to: Microsoft, Solaris and Linux Operating System, Mainframe (Z/OS), Oracle database, Cisco for wired and wireless Local Area Networks (LANs) and Wide Area Networks (WANS).
- Personnel must perform the testing and document the significant findings in the Security Test and Evaluation report. The documentation must include summary of findings, impact of finding, and recommendations for fixes or other security mitigation strategies.

### **3.7 Task Area 7 - General Tasks**

**3.7.1 Capability Maturity Model Integrated (CMMi):** The contractor shall work in conjunction with the overall CBP effort to achieve an evaluated, Level 3 integrated CMMi rating, capitalizing on the overall management and direction that shall be provided through the contract support provided for the overall CMM effort. The contractor shall identify those areas of the CMM to be included in the CMM effort and ensure that the appropriate processes and practices are included and addressed. This includes supporting the overall effort by participation in process action teams and working groups and through the development or updates of templates, processes, profiles, procedures, practices or other work products that will support security engineering and execution within CBP.

**3.7.2 Compliance Measurement:** As documented in the Customs Information Systems Handbook (CIS HB) 1400-05B, CBP Security Policy and Procedures

Handbook, and as part of CMM process improvement, the contractor shall assist in the development of metrics appropriate to measure the compliance and state of the CBP security posture and the effectiveness of the audit, assessment and documentation implementation and compliance.

**3.7.3 Communications Plan:** The contractor shall develop a plan that includes tailored delivery of the CBP security message while establishing the expectation for compliance and the consequences for noncompliance. The communications plan shall be the vehicle to deliver the security message as it relates to areas such as: policy and procedures, architecture, training and incident identification and reporting. The contractor shall utilize all available means to communicate the necessary information, to include: conferences, conference calls, meetings, committees and incorporation into performance evaluation.

**3.7.4 Subject Matter Experts for Training:** The contractor shall provide subject matter expertise to the Office of Training and Development (OTD). The training material shall be in support of computer security awareness and security practices for all CBP employees and contract personnel involved with operation of computer systems. This support shall include assistance in the creation, evaluation and review of content for training materials.

#### **4.0 Deliverables**

##### **4.1 Reports**

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. In addition, deliverables shall be clear and concise; with engineering terms and project management tools used, where appropriate. All graphics shall be easy to understand, properly labeled with legends and be relevant to the supporting narrative. Deliverables must conform to the On-Site Technical Managers' (OTMs') (i.e., Government Team Leads') specifications. The contractor shall provide the COTR and OTM with a copy of all report deliverables furnished under this task order in soft copy via e-mail.

##### **4.2 Status Reports**

###### **4.2.1 Weekly Reports**

The written weekly report shall consist of a summary of significant events and actions accomplished for the week. A bi-weekly verbal presentation shall consist of the following: actions accomplished for the previous two-week period; actions planned; and any issues of concern that may require special attention. This verbal report shall be presented to the Chief, STP Branch, COTR, and the OTMs on the second and fourth Thursday or as otherwise scheduled by the COTR.

#### **4.2.2 Monthly Report**

The contractor shall submit monthly status reports to the COTR and OTMs on progress made during the respective reporting period in performance of the work requirement. The reports shall address work completed during the current period, planned activities, problems/issues with recommended solutions, anticipated delays, and resources expended. The reports shall be sufficiently detailed to provide an ongoing record of all support efforts.

These reports 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 monthly report shall be delivered in hard copy to the COTR and OTMs. One electronically provided (i.e., via email) soft copy shall be sent to the COTR. The report shall be in a format to be agreed upon with the COTR.

#### **4.2.3 Cost Reports/Invoices**

To ensure the timely processing of the contractor's invoices, the contractor shall provide the COTR with copies of timesheets at the end of each timesheet period for each person with hours expended in support of the contract over the reporting period.

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 the 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 and 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."

#### 4.2.4 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. One (1) copy of the invoice document shall be submitted to the COTR at the following address:

U.S. Customs and Border Protection  
7451-A Boston Boulevard, NDC4 Cube 66  
Springfield, Virginia 20598  
Attn: (b) (6)

Simultaneously, one copy of the invoice shall be mailed to the Contracting Officer at the following address:

U.S. Customs and Border Protection  
Office of Finance, Procurement  
ATTN: (b) (6) Contract Specialist  
1331 Pennsylvania Avenue, NW, Rm 1301  
Washington, DC 20229

#### 4.2.5 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.

#### **4.2.6 ODC Process**

The contractor shall acquire the COTR or his/her designee's approval on all ODCs prior to initiating any purchase and/or 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.

#### **4.2.7 Travel**

All 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 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).

Travel expenses shall be separately identified on invoices accompanied by all paid receipts during the time of travel.

#### **4.3 Briefings and Meetings**

Each briefing/meeting shall cover the essential elements of the relevant subject matter and shall be prepared and presented in a clear, concise, and orderly manner. Appropriate briefing tools such as Microsoft PowerPoint, 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.

##### **4.3.1 Meetings**

- a. Kick-Off Meeting/Draft Project Schedule – A task order kick-off shall be scheduled within 10 days after award. Attendees shall be at a minimum: CBP COTR, On-Site Technical Managers (OTMs), Contracting Officer, Program Manager and contractor. The contractor shall provide a draft schedule of their plan to meet the customer's requirements as identified in this statement of work. This shall be due within 10 workdays after award of the task order. Any changes or adjustments to this schedule shall be coordinated with the appropriate OTM.
- b. Periodic Meetings: CBP will coordinate periodic meetings and reviews to ensure all relevant provisions of the task order are being met.

#### **4.4 Performance**

The contractor shall follow the performance guidelines listed below.

#### 4.4.1 Place of Performance

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

#### 4.4.2 Hours of Operations

All work shall be performed during a normal 40-hour week -- Monday through Friday, with core hours from 9:00 AM until 3:00 PM. Core hours refer to the hours of the day contractors shall work. The contractors shall begin work no later than 9:00AM. The contractor can start earlier than 9:00 AM but shall not end their day earlier than 3:00PM. Contractors shall take at least 30 minutes for lunch. For example, a contractor must spend 8 hours and 30 minutes at work to claim an 8-hour day.

The technical staff shall work on-site at the government facility unless approval is obtained from the COTR. The contractor staff shall observe the following government holidays unless the COTR approves otherwise:

- Christmas
- New Year's
- Martin Luther King
- President's Day
- Memorial Day
- Independence Day, July 4<sup>th</sup>
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day
- Inauguration Day (as appropriate)

The contractor staff shall inform the OTMs of all vacations and other time off. The contractor staff shall provide adequate coverage (as determined by OTMs) on all business days – to include weekdays after holidays.

#### 4.4.3 Period of Performance

Base Period	01/01/07 thru 12/31/07
Option Period #1	01/01/08 thru 12/31/08
Option Period #2	01/01/09 thru 12/31/09
Option Period #3	01/01/10 thru 12/31/10
Option Period #4	01/01/11 thru 12/31/11

#### 4.5 Delivery Schedule

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
1	Kick-Off Meeting/Draft Project Schedule	4.2.a	Within 10 days after award	Within 10 days of award	OTMs, COTR and Contractor Project Manager
2	Security Assessment Reports	3.1.1	As Required	As Required	COTR, applicable OTM
3	Privacy Impact Assessment (PIA)	3.1.2	As Required	As Required	COTR, applicable OTM
4	E-Authentication	3.1.2	As Required	As Required	COTR, applicable OTM
5	Controls Testing (Security Test and Evaluation (ST&E)) Plan and Results	3.1.2	As Required	As Required	COTR, applicable OTM
6	System Security Authorization Agreement (SSAA) for CLASSIFIED Systems	3.1.2	As Required	As Required	COTR, applicable OTM
7	Authorization to Operate (ATO) Letter	3.1.2	As Required	As Required	COTR, applicable OTM
8	Self Assessment (NIST SP 800-26)	3.1.2	As Required	As Required	COTR, applicable OTM
9	FIPS-199 Assessment	3.1.2	As Required	As Required	COTR, applicable OTM
10	Risk Assessment	3.1.2	As Required	As Required	COTR, applicable OTM
11	System Security Plan	3.1.2	As Required	As Required	COTR, applicable OTM
12	Contingency Plan	3.1.2	As Required	As Required	COTR, applicable OTM
13	Contingency Plan Test Results	3.1.2	As Required	As Required	COTR, applicable OTM
14	C&A Artifacts and documentation as specified by DHS and/or CBP requirements	3.1	As Required	As Required	COTR, applicable OTM

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
15	Updated COMSEC Account Database Reports	3.2.1	As Required	As Required	COTR, applicable OTM
16	COMSEC Training - Soft copy of training materials	3.2.2	As Required	As Required	COTR, applicable OTM
17	Documentation and Reports regarding COMSEC Custodian appointments and COMSEC Accounts	3.2.2	As Required	As Required	COTR, applicable OTM
18	Technical Reference Model (TRM) ESSC Catalog Updates and Design Improvements Documentation and Progress Reports	3.3.1	As Required	As Required	COTR, applicable OTM
19	Policy Guides and Handbooks	3.4.1	As Required	As Required	COTR, applicable OTM
20	Section 508 Training Materials	3.4.2	As Required	As Required	COTR, applicable OTM
21	Risk Assessment Security Questionnaire	3.5	As Required	As Required	COTR, applicable OTM
22	Risk Assessment Visit Plans and Process Documentation	3.5	As Required	As Required	COTR, applicable OTM
23	Risk Assessment Reports	3.5	As Required	As Required	COTR, applicable OTM
24	Plans of Action and Milestones Documents	3.5	As Required	As Required	COTR, applicable OTM
25	Security Test and Evaluation Reports	3.6	As Required	As Required	OTM TPOC
26	Communications Plan	3.7.3	As Required	As Required	COTR, applicable OTM

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
27	Content for Training/Review of Training Material	3.7.4	As Required	As Required	OTM TPOC
28	Weekly Reports	4.2.1	Weekly	Weekly	COTR, applicable OTM
29	Monthly Reports	4.2.2	Monthly	Monthly	COTR, applicable OTM
30	Cost Reports	4.2.3	Monthly	Monthly	COTR, applicable OTM

The work products are to be delivered in accordance with the schedule set forth in the table above. All documents must be provided in soft copy format to the recipients listed above. In addition, one hard copy should be provided to the OTM. The contractor shall refer to Section 4 Deliverables for work product

#### 4.6 ACCEPTANCE REQUIREMENTS

The on-site technical manager (OTM) shall review all deliverables for accuracy and completeness. The contractor shall make those corrections required by the OTM. The deliverables require acceptance by the appropriate OTM or the COTR.

##### 4.6.1 General Acceptance Criteria

Specific criteria shall be set forth for each task area, if applicable. Accordingly, general quality measures, as set forth below shall be applied to each work product received from the contractor under this SOW.

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 SDLC-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.

#### 4.6.2 Points of Contact

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

**CBP, COTR**

U.S. Customs and Border Protection  
7451-A Boston Boulevard, NDC4 Cube 66  
Springfield, Virginia 20598  
Attn: (b) (6)

**OTM:**

On-site Technical Managers STP

(b) (6)

#### 5.0 ACCESSIBILITY REQUIREMENTS

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 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, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then “1194.21 Software” standards also apply to fulfill functional performance criteria.

36 CFR 1194.25 – 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.

36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) 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 DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

36 CFR 1194.2(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 of 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.

### 6.0 Level of Effort (Project Staffing Estimates)

The following estimates are for planning, proposal pricing and evaluation purposes.

Labor Category	FTE	Estimated Hours by Labor Category
Project Manager	1	1,920.00
Subject Matter Expert	1	1,920.00
Technical Writer/Editor	2	3,840.00
Administrative Specialists (Senior)	2	3,840.00
IT Security Specialist (Senior)	12	23,040.00
IT Security Specialists	17	32,640.00
Computer Systems Analyst (Senior)	9	17,280.00
<b>Total</b>	<b>44</b>	<b>84,480.00</b>

### ADDITIONAL CONTRACTOR PERSONNEL REQUIREMENTS

*The Contractor will ensure that its employees will identify themselves as employees of their respective company while working on U.S. Customs & Border Protection (CBP) contracts. For example, contractor personnel shall introduce themselves and sign attendance logs as employees of their respective companies, not as CBP employees.*

*The contractor will ensure that their personnel use the following format signature on all official e-mails generated by CBP computers:*

*[Name]  
 (Contractor)  
 [Position or Professional Title]  
 [Company Name]  
 Supporting the XXX Division/Office...*

*U.S. Customs & Border Protection*  
*[Phone]*  
*[FAX]*  
*[Other contact information as desired]*

## **Enterprise Architecture (EA) 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 DHS Homeland Security HLS () EA and the CBP EA.

All IT hardware or software shall comply with the HLS EA and the CBP 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 (DEB) and the CBP Enterprise Architecture Branch (EAB).

**IPv6 Clause:**

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. All Information Technology assets being developed, procured, or acquired shall be IPv6 capable

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

- **DHS Accessibility Requirements Tool (DART)**

**(b) (7)(E)**

Utilize this tool to determine the 508 compliance clauses to include in the SOW.

**ISO (Information Security) COMPLIANCE**

- **Information Security Clause: (include at the End of the Security section)**

"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.

- **HSAR Clauses to Include in the SOW/Contracts – as of March 22, 2007**

**3052.204-70 Security Requirements for Unclassified Information Technology Resources (JUN 2006)**

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

**Comment [AU1]:** "its" shows possession, "it's" is the same thing as "it is." -- "its" refers to the "contractor's IT Security Plan."

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged

from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(f) DHS MD 4300.1 *Information Technology Systems 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**

The following requirement should be incorporated into all acquisition documents:

**OMB-M-07-18 FDCC**

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.

(End of clause)

**3052.204-71 Contractor employee access.**

As prescribed in (HSAR) 48 CFR 3004.470-3(b), insert a clause substantially the same as follows with appropriate alternates:

**CONTRACTOR EMPLOYEE ACCESS  
(JUN 2006)**

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

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

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

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

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed

forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

**ALTERNATE I  
(JUN 2006)**

When the contract will require contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of

violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

**ALTERNATE II  
(JUN 2006)**

When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for

permanent residence as evidenced by a Permanent Resident Card (USCIS I-55 1). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

- **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.

- **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), CBP ISSM, 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.

## **Engineering Platforms**

**Common Enterprise Services (CES)** – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. This includes the build out and integration of all required services and infrastructure, which must include the Single Sign-on Portal and CBP Enterprise Services Bus (ESB), required for the CES. Capabilities shall be designed to the DHS standard operating architecture (SOA), transportable between DHS data centers (CBP National Data Center, Stennis, and DHS 2<sup>nd</sup> data center).

**Single Sign-on Portal** – Design, build, and operate a single sign-on Portal - consistent with DHS' enterprise portal solution (for which ICE is the steward) - to provide a common point of access, with a single sign-on capability to existing applications and to provide the infrastructure for integrating diverse internal and/or external information and transactional resources. This includes the migration of the current ACE Portal to the Single Sign-on Portal as rapidly as feasible.

## **Portfolio**

**This acquisition request aligns to the following primary DHS IT Portfolio:?**

### **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).