

Statement of Work (SOW)

For

Information Technology Training & Support Services

HSBP1010F00356 Attachment 1

7/1/2010

Information Technology Training & Support Services

Table of Contents

| | | |
|-----|--|----|
| 1. | BACKGROUND | 3 |
| 2. | SCOPE | 4 |
| 3. | APPLICABLE DOCUMENTS | 4 |
| 4. | SPECIFIC TASKS..... | 5 |
| 5. | DELIVERABLES AND DELIVERY SCHEDULE | 7 |
| 6. | GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION | 12 |
| 7. | PLACE OF PERFORMANCE | 15 |
| 8. | PERIOD OF PERFORMANCE | 16 |
| 9. | SECURITY | 16 |
| 10. | SPECIAL CONSIDERATIONS..... | 18 |

Information Technology Training & Support Services

1. BACKGROUND

The United States Customs and Border Protection, (CBP) was established as one of the three operational agencies within the Border and Transportation Security Directorate of the Department of Homeland Security (DHS). CBP consists of the inspection and frontline border enforcement functions of the U.S. Customs Service, the Immigration and Naturalization Service (INS), including the Border Patrol, and the Animal and plant Health Inspection Service (APHIS). It also includes all the trade and revenue collection function of the U.S. Customs Service. The predecessor agencies each have rich histories and missions that they bring to CBP. But today, as part of the historic creation of a unified agency, the priority mission of all CBP personnel is to detect and prevent terrorists and terrorist weapons from entering the United States.

http://www.cbp.gov/xp/cgov/toolbox/about/mission/cbp_plans_reports.xml

In the process of accomplishing this mission, Customs clears more than 14 million cargo shipments per year, collects more than \$20 billion in revenue, processes more than 12 million formal entries, of which approximately 55 percent involve merchandise subject to quota or other trade programs, and monitors an average of 10 million annual export shipments. In 2007, CBP inspected 411 million passengers, 120 million vehicles and other modes of transportation, arrested 25,000 suspected criminals, seized more than 820,000 pounds of narcotics, interdicted more than 170,000 inadmissible aliens, and conducted 1.5 million agriculture interceptions. This broad mandate encompasses a wide range of law enforcement activities and responsibilities, supported by expansive, state-of-the-art computer systems, tactical communications equipment, and technology equipment such as in-ground sensors, cameras, and non-intrusive inspection equipment. This broad mandate encompasses a wide range of law enforcement activities and responsibilities, supported by expansive, state-of-the-art computer systems.

Approximately 55,000 full-time CBP employees support the CBPs' mission at over 1800 field locations, multiple locations along the border between designated ports of entry, air and marine facilities, and at its Headquarters in Washington, DC.

The Enterprise Network and Technology Support Division (ENTS) are responsible for enterprise architecture, design and management of CBP network infrastructures, including the shared departmental DHS OneNet. ENTS provides operational day-to-day technology support to all CBP field locations, technology training, enterprise wide area network, security operations and helpdesk services. ENTS provides reliable and responsive technology systems, tools and services in unwavering support of the CBP mission to protect our nation with goals of improved availability of critical systems, improved customer satisfaction and increased integration across teams and technologies.

In order to support this mission, approximately 13,000 students in 550 classes are trained each month. Additionally over calendar years 2005 thru 2009, 550 deliverables were provided to

support these training efforts utilizing contractual support. ENTS Technology Training trains all customers of CBP systems which include more than 30 government and state and local agencies.

2. SCOPE

The Contractor shall provide services to support the management process of technical programs identified in this Statement of Work (SOW). The Contractor shall provide qualified personnel with the expertise required to support the CBP and shall adhere to the following guidelines:

- Plan, prepare and present for the orderly transition of work from the incumbent to the new contract, and work with the Government personnel in implementing this plan.
- Proposed personnel shall have successfully completed CBP background investigation.
- Proposed personnel may be required to travel nation-wide, as well as internationally to support requirements.
- Furnish, as required, training support personnel and services to assist the CBP in developing and providing training to users of all automated systems and platforms supported by the CBP, including: Microsoft applications; computer and web-based; and, interactive distance learning training.
- Furnish, as required, training support personnel and services to assist the CBP in developing and providing training to users of tactical radio and communications equipment supported by the CBP, including: training for the maintenance of information technology (IT) systems and enforcement technology.
- Follow the prescribed policies, life cycles, and standards of the Customs Systems Life Cycle (SLC) in developing, maintaining, or implementing information and technology projects and systems.
- Consistent support to the process management and quality improvement activities of CBP.
- Matrix staff to tasks to identify availability of resources through the life of the contract.
- The *System Life Cycle (SLC) Handbook* (b)(2), (b)(7)(E) describes the official CBP policy that applies to all Information and Technology (IT) projects and systems.
- Apply concepts and techniques of organizational improvement as defined by the Software Engineering Institute (SEI) and characterized by the *Capability Maturity Model (CMM)*. Utilize the following link for reference:
<http://www.SEI.CMU.edu>

3. APPLICABLE DOCUMENTS

HB 1400-05D CBP Information Systems Security Policies and Procedures Handbook

- Version 1.1
- July 27, 2009
- Section 4.1.5.1 Initial Awareness
- Section 4.1.5.2 Refresher Awareness
- (b)(2), (b)(7)(E)

DHS 4300A Sensitive Systems Handbook

- Version 7.1
- November 13, 2009
- 4.1.5.1 Initial Awareness
- 4.1.5.2 Refresher Awareness
- 4.1.5.4 Role-Based Training
- (b)(2), (b)(7)(E)

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

3052.204-71 Contractor employee access as prescribed in (HSAR) 48 CFR 3004.470-3(b), i

OAST (Office on Accessible Systems and Technology) Compliance DHS Accessibility Requirements Tool (DART)

(b)(2), (b)(7)(E)

4. SPECIFIC TASKS

The OIT Program Offices were created to deliver modern, integrated science and technology solutions to support the CBP mission. Through these offices, OIT transforms CBP information technology systems and supporting infrastructure into a fully integrated, interoperable, architecture-based environment while maintaining the highest standards of service to customers. All Program Office training teams shall be responsible for the reoccurring Instructor Led-Training, ILT's and specific requirements related to these training classes noted in Section five such as research, design, development of ILT documentation, and maintenance of current documentation such as Instructor guides and user guides. All training requirements are listed below in sections four and five with the exception of Just-in-Time training which is not noted. However, in the previous year 60 Just-in-Time ITL training sessions were provided across the United States. ENTS Technology Training provides training support to the Program Offices which are defined below:

- The Passenger Systems Program Office (PSPO) provides application development and continued operational support of all passenger and immigration management systems hosted by CBP. Some of the Passenger Systems/projects include the Treasury Enforcement Communications System (TECS), the Advanced Passenger Information System (APIS), the Global Enrollment System (GES), the Integrated Automated Fingerprint Identification System (IAFIS), The United States Visitor and Immigrant Status Indicator Technology Program (US-VISIT), the Outlying Area Reporting System (OARS), and the Private Aircraft Reporting System (PARS).
 - The current schedule for PSPO consists of 113 ILT training sessions across the United States.
- The Border Enforcement & Management Systems Program Office (BEMS) is responsible for the full system development life cycle planning through deployment of all Border

Enforcement, Mission Support, and information dissemination systems. Some of the BEMS Systems/projects include the Seized Asset and Case Tracking System (SEACATS), the TECS Case Management system, the Enforcement Integrated Database (ENFORCE), the Border patrol Enforcement Tracking System (BPETS), the CBP Overtime Scheduling System (COSS), the CBP Automated Travel SYSTEM (CATS), Remedy Asset Management and the Systems, Applications and Products System (SAP).

- The current schedule for BEMS consists of 92 ILT training sessions across the United States.
- National Training Plan - Tactical Radio and Communication Training (TRaCT) provides training to CBP and numerous partner agencies utilizing the Land Mobile Radio network based out of the National Law Enforcement Communications Center. TRaCT provides training through the use of an Inter-agency agreement (IAA) with ICE: TTSP's (TRaCT) has been gearing up for phase II of the AZ P25 upgrade project (vote-scan) which will require the training of approximately 3,000 officers. On the schedule to be trained is El Paso, Houlton and Swanton projects this year (another 4000+ users). Additionally, OFO is deploying 3,500+ radios to their officers in the next ten months with a mandatory training requirement. TRaCT provides continual refresher training (3,000+ yearly) supporting OBP. TRaCT has training requests and plans to train over 13,000 CBP personnel this year. This training is a high priority because of the unique officer-safety and emergency interoperability communication requirements. This training enables the use of radios to provide essential law enforcement information in a secure environment and is available in many areas where secure cellular telephone service is not available.
 - The current class schedule for Tactical Radio is 85 ILT sessions for the year.
- The Computer Security Team (CST) provides mandatory TECS privacy awareness and general privacy awareness training and the development of Security Awareness and Rules of Behavior Training and the TECS moderation project training development efforts. The CST team provides training to CBP and 26 other federal agencies that rely on CBP to provide TECS, NCIC, NLETS, ACS and TECS/ACS SCO Training. This group also maintains and manages access to the TPA and GPA training that enables all authorized personnel to have access to the Mainframe systems and applications. This group also provides Technology Support Desk Tier II and Tier III support for TECS and resolves about 700 service and incident request a month for the 27+ federal plus state and local agencies utilizing the TECS system.
 - The current class schedule is 96 ILT session schedule for this year.
- The Distributive Learning Team (DLT) is responsible for the development and design of the web-base training classes. The primary course the DLT team supports with development and Virtual Learning Center (VLC) compliance is the Computer Security and Rules of Behavior mandatory annual training.
 - This group shall utilize subject matter experts from each group and create story boards, graphic designs and graphic animation to develop and finalize web-based training courses for the Virtual Learning Center, (VLC).
 - Twenty five classes have been identified to be placed into the VLC.
- Field Technology Instructors provide training in current and newly developed high priority projects such as IE8, Modernization projects and just-in-time training. This group provides personnel to complete Operation Manuals, training manuals, user guides, and assist with the develop Web Based applications training. This group is positioned at

key locations to provide local support to the DFO, Sector, Station, OAM office, and Field Support to provide technology training support within their designated area of operation and travel as needed to support deployments nation-wide.

- The current ILT FTI class schedule is 72 ILT sessions for the year.
- The FTI's also provide support to desktops customers and users and resolves those incidents or requests requiring assistance with desktop applications.
- Global Online Support – Technology Service Desk (TSD) Advanced GOES support provides external training and support that promotes travel to the United States. This group receives and resolves about 2,500 requests a week in support of Global Online Enrollment System. This group is required to provide support during core business hours across the United States, these hours are currently 1000 to 1800 and are subject to change. Some of these requests are noted below.
 - Service Requests from Applicants in GOES.
 - Health checks
 - Maintain and gather SOPs, FAQs, Knowledge Base that pertain to applications and associated info with incoming calls to improve Tier 2 functionality
 - System Security more in depth users account issues, new accounts, suspension removals, recertification, maintenance of user profiles
 - Account creations
 - Reset passwords.
 - Assistance in completion of applications in multiple languages.

CBP Automated Environment

CBP is a leader among Federal Government agencies in its use of state-of-the-art automated systems technology to support its mission. In addition to four mainframe processors, CBP sites are interconnected by Local Area Networks (LANS), and have access to the Internet as well as to the CBP Intranet site.

The OIT Technology Training and Support Program Office has the responsibility of ensuring that the CBP workforce is trained to effectively make use of advanced technological capabilities to support its many public service commitments.

For a detailed description of the computer resources used by the CBP, log on to its web site at www.cbp.gov. From the home page the path is ***Procurement and contracts/Customs Modernization/Bidders Library/Current Systems.***

5. DELIVERABLES AND DELIVERY SCHEDULE

The contractor shall ensure that all training documentation listed below are maintained and kept current with any changes within the applications. The Contractor shall provide training support personnel and services to assist in the following major areas:

- Design, delivery, and evaluation of training programs.
- Development of courseware, online help and end-user documentation
- Support of automated systems and creation and maintenance of data used for training.

- Generation of weekly and monthly status reports, and Ad Hoc reports.
- Documentation such as but not limited to:
 - User/Customer Assistance Guides.
 - Quick Reference Guides.
 - Instructor Guides.
 - Documentation Quality Assurance.
 - Customer Support.

Training Design and Delivery

The Contract shall apply Instructional Systems Design (ISD) practices and principles to tailor course content and instructional methods to the requirements of the users.

The Contractor shall apply the principles embodied in the Capability Maturity Model (CMM) to the development of new training programs or the modification of existing programs. Training plans shall address all activities of the SLC, include milestones, identify resources for successful completion of each task, and define metrics to be used to measure the effectiveness of the training.

The Contractor shall administer the training using a variety of methods, which include but are not limited to the use of multimedia software, distance learning, interactive training techniques, and Web-Based Training (WBT) methodologies.

An entrance and exit transition plan shall be included with proposal by the Contractor to ensure smooth transition between Contractors.

Labor rates proposed shall be nation-wide; at a minimum for: the Washington Metropolitan area; Laguna Niguel/Long Beach, CA; Tucson, AZ; Indianapolis, IN; Orlando, FL; Brunswick, GA; Harpers Ferry, WV; Artesia NM; and Colorado Springs, CO.

The Contractor shall provide qualified personnel to assist government personnel in carrying out the following categories of tasks:

Assessment of Training Needs of End-Users

The Contractor shall work closely with the CBP staff, the Field Training Coordinator, user groups, and technical personnel to define training requirements. Based on an analysis of these requirements the Contractor shall assist in the development of business cases to verify and validate the procurement and/or development of new training programs. This may include the development of cost/benefit analyses associated with the business cases.

Evaluation of Training Methodologies and Technologies

The Contractor shall be knowledgeable of training solutions that employ state-of-the-art technologies and shall make recommendations to the government for training strategies that will meet the requirements of the users and include technology-based alternatives to conventional,

instructor-led training. Included with each recommendation will be a cost/benefit analysis or basis of estimate.

Design and development of Training Courses

In conjunction with CBP Staff, the Contractor shall design and develop new training courses and/or modify existing training courses. As part of this activity the Contractor shall perform the following types of tasks:

Based on user requirements, develop a detailed functional design specification for the training program.

Recommend training approaches that are cost-effective and best-suited to the needs of the users, including but not limited to interactive courseware such as CBT or Web-Based Training (WBT).

Delivery of Training Methods

The Contractor shall be capable of delivering training using all of the following methodologies and provide specific services:

- Instructor-led classroom training
- Computer-based training (CBT)
- Web-based training (WBT)
- Interactive distance learning (IDL)
- Electronic online help
- Hands-on communication equipment training
- IT equipment maintenance training

The emphasis in all training programs shall be on the concepts and skills needed by CBP employees to maximize productivity by effectively making use of the all available resources. Computer training may relate to any application system, equipment, or to the PC/LAN software used by the CBP.

The Contractor shall conduct training at local sites within the Washington, DC metropolitan area, and field sites throughout the United States (including its territories and possessions), and international sites.

Evaluation of Training Effectiveness

The Contractor shall assist in utilization of automated tracking and evaluation tools to measure the effectiveness of training programs. The tools used will include, but not be limited to, questionnaires, course evaluation forms, and user surveys. Incorporated in this analysis will be comparisons of the cost and effectiveness of various training methodologies.

Providing Administrative Support

The Contractor shall assist the CBP Staff in the scheduling of training courses, the registration of participants, the scheduling of resources for the training programs, and the entry and maintenance of training statistics in an automated tracking system. As part of this activity, the Contractor shall perform the following tasks:

- Prepare course schedules for dissemination to users.
- Notify course attendees of information pertinent to the course.
- Schedule training rooms and ensure that they are properly equipped and set up for the training sessions.
- Prepare course materials in the format required for the training, provide quality assurance on all prepared documentation, including uploading online help and online manuals to mainframe, SharePoint and servers; copying training materials to disk for mass distribution; and the preparation of printed materials.
- Enter statistical information about the training courses into various automated tracking systems.
- Monitor and provide information to CBP staff regarding usage and problems.
- Assist CBP employees with using and troubleshooting learning systems.

Development of Training Courseware and User Documentation

The Contractor shall assist the CBP in the development of course materials, instructional aids, and user documentation to reinforce the transfer of information. Templates of formats and styles to be utilized for training material can be found in attachment A.

Training Courseware

The Contractor shall develop training courses in a format which best meets the learning needs and characteristics of the target audience and the training content. The courseware may take the form of, but is not limited to, interactive modules, user guides, courses manuals, quick reference guides, training information embedded within application, instructor manuals, demo disks, and online tutorials. The delivery method may employ both conventional and alternative media.

User Documentation

The Contractor shall provide support to CBP staff in the review, edit and rewrite of the CBP handbooks and instructional guides prepared by subject matter experts. The Contractor shall provide support in the development of online help, online user manuals, and documentation embedded within computer applications. The documentation shall provide the user with clear, concise instructions on how to use the application or equipment. The Contractor shall make use of the methodology and media best suited for conveying the information to the users. The documentation may be presented in an electronic format, as written material, as a video presentation, or in any combination of these.

Provide Automated Data Processing Technical Support

For each of the major computer application systems and automated training area exists on the mainframe or servers where users can learn how an application works without being in the live production environment. The primary purpose of these training systems is to facilitate structured hands-on practice and training, either in a classroom setting, individual basis or alternative training platforms. The Contractor shall provide technical support services for the maintenance and administration of these automated training systems. The types of tasks the Contractor shall perform include, but are not limited to:

- Development of functional requirements for enhancements to the automated training environment.
- Development of program specifications for reports and other outputs required by CBP management.
- Development of software requirements for the interface between commercial off-the-shelf (COTS) and CBP application systems.
- Modification of software and/or databases, as required to run applications in the training environment.
- Coordination with the Program Offices to ensure that the training system accurately represents the production environment.
- Analysis and comparison of training-related software alternatives to determine which products most closely satisfy user needs and meet system requirements.
- Provide equipment/network troubleshooting services to OIT Field Technology Offices.
- Creation and maintenance of training data and training logons.

CBP Mission or Application Systems to Support

The Contractor shall provide training and consulting support not limited to the following:

- Border Unification training
- Advance Passenger Information System training
- US Visit – Land Borders training
- US Visit – Air and Sea training
- SBI Net
- Consular Consolidated Database
- Trusted Traveler Documentation
- COSS (Payroll)
- Seized Assets and Case Tracking System (SEACATS)
- Integrated Automated Fingerprint Identification System (IAFIS)
- Free and Secure Trade Initiative
- Automated Commercial Environment (ACE)
- Customs Airborne Stabilized Optical System (CAOS)
- Automated Targeting System (ATS)
- Computer Emergency Response Team (CERT)
- Internal Customs-Trade Partnership Against Terrorism (C-TPAT)
- Office of Training Development
- Cargo Management Systems Office

- Passenger Management Systems Office
- Wireless Land mobile network infrastructure and equipment
- Installation and maintenance of CBP equipment

The Contractor shall submit a weekly, electronically prepared status report which identifies and describes ongoing, as well as upcoming activities; accomplishments; planned and completed travel; recommendations for problem resolution.

| | |
|---------------------|----------------------------------|
| Deliverables | Status Report |
| Performance Dates | Weekly |
| Acceptance Criteria | 99% submission of status reports |

Monthly Status Report

The Contractor shall submit monthly status reports, either type written or in electronic format, to the COTR on a schedule to be determined by the COTR. These status reports shall contain significant functional accomplishments, meeting attended, courses conducted, problems and unresolved issues, and objectives for the subsequent week. The COTR has ten workdays to review and approve reports. The Contractor shall have five workdays to correct any report as requested by the COTR.

Quarterly Status Reports

The Contractor shall submit cumulative status reports for all contract staff, on a quarterly basis, either type written or in electronic format, along with the invoice of billable hours. Format and content of reports will be submitted to COTR for review and approval. The COTR will request in writing 30 days in advance of any modifications to the reports.

6. GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION

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.

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 S SI," 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, and 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.

(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.

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:

(m) 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.

(n) 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.

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.

7. PLACE OF PERFORMANCE

Location: Work shall be performed primarily at the CBP Lorton facility 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
10720 Richmond Highway, Suite A
Lorton, VA. 22079

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 from 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.

Travel and per diem rates for reimbursement purpose shall be in accordance with acceptable accounting procedures and Federal Acquisition Regulation (FAR) 31.205-46.

The Contractor shall be reimbursed by the Government for travel costs required in performance of this contract provided such travel has the prior approval of the Contracting Office. Request for travel shall be in writing and shall include the dates, locations, and estimate costs of the travel. Some travel may require passport for international travel.

The Contracting Office will provide authorization under FAR Subpart 51.2 (Contractor Use of Interagency Fleet Management System (IFMS) Vehicles)
http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/far/51.htm#P78_9951
for the Contractor personnel to utilize Government owned vehicles for specific tasks.

Travel for trainers and staff will be required in this task to perform duties. Travel is based on trainers and area analyst who travel at least two weeks a month.

8. PERIOD OF PERFORMANCE

The period of performance under this task order is 7/2/2010 through 7/1/2011.

9. SECURITY

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.

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. MIIA-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 (WGM), 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 WGM 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 WGM 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.

Identification Badges

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

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]

10. SPECIAL CONSIDERATIONS

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

CBP, COTR

(b) (6)

Director, Technology Training & Support Program
Enterprise Networks and Technology Support Division
OIT, USCBP, DHS
10720 Richmond Highway, Suite A
Lorton, VA. 22079

(b) (6)

ACCESSIBILITY REQUIREMENTS (SECTION 508)

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 (EIT), 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 EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

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

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

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.

Section 508 Applicable Exceptions

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 1194.3(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.

Section 508 Compliance Requirements

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 meet 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 authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.