

**Statement of Work (SOW)**

**For**

**Information Technology Training & Support Services**

**HSBP1010F00519**

**Attachment 1**

**9/16/2010**

Information Technology Training & Support Services

Table of Contents

- 1. BACKGROUND ..... 3
- 2. SCOPE ..... 4
- 3. APPLICABLE DOCUMENTS ..... 5
- 4. SPECIFIC TASKS..... 6
  - 4.1 Maintenance of Existing ACE and Legacy Training Materials..... 6
  - 4.2 Development and Delivery of New ACE Curriculum..... 7
  - 4.3 Account Services Desk ..... 8
  - 4.4 Client Representative Support ..... 8
  - 4.5 Tactical Radio and Communication Training (TRaCT) ..... 9
  - 4.6 Assessment of Training Needs of End-Users ..... 10
  - 4.7 Evaluation of Training Methodologies and Technologies ..... 10
  - 4.8 Design and development of Training Courses..... 10
  - 4.9 Evaluation of Training Effectiveness..... 10
  - 4.10 Providing Administrative Support ..... 10
  - 4.11 Training Courseware..... 11
  - 4.12 User Documentation ..... 11
  - 4.13 Provide Automated Data Processing Technical Support ..... 11
  - 4.14 Anticipated Staffing Levels, Labor Categories, Travel, and Other Direct Costs (ODCs) ..... 12
- 5. DELIVERABLES AND DELIVERY SCHEDULE ..... 12
- 6. GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION ..... 15
- 7. PLACE OF PERFORMANCE ..... 16
- 8. PERIOD OF PERFORMANCE ..... 16
- 9. SECURITY ..... 16
- 10. SPECIAL CONSIDERATIONS..... 21

## 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/about/mission/guardians.xml>

In the process of accomplishing this mission, CBP 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.

Approximately 55,000 full-time CBP employees support the CBP's mission at over 1,800 field locations, multiple locations along the border between designated ports of entry, air and marine facilities, and at its Headquarters in Washington, DC.

The CBP Office of Information and Technology (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.

The Enterprise Network and Technology Support Division (ENTS) is 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.

CBP is modernizing the business processes essential to securing U.S. borders, speeding the flow of legitimate shipments, and targeting illicit goods that require scrutiny. The key technology driver of this activity is the development and deployment of the Automated Commercial Environment (ACE). In addition to the development and delivery of the ACE system, the ACE program is also responsible and for the development, delivery, and maintenance of all ACE-related and legacy cargo processing systems-related training.

The Contractor shall provide staff to work alongside Government personnel and shall use the Instructional System Design (ISD) framework and methodologies to prepare system customer and user training for new ACE releases. The contractor shall also be responsible for the maintenance of existing cargo-related courses. As the training provided will focus on CBP, trade community and Participating Government Agency (PGA) audiences, the Contractor should have knowledge of international trade laws and regulations, CBP processes, and integration with PGAs.

Table 1-1 is representative of CBP instructional materials. Additional instructional materials may be identified by CBP to support agency needs.

**Table 1-1: CBP Instructional Materials**

<b>Method</b>	<b>Materials Included (but not limited to)</b>
Instructor Led Training (ILT)	Concept Slides
	Student Guides
	Instructor Guides
	Interactive System Simulations (currently in Captivate and Flash format)
	Quick Reference Guides (QRGs)
	Training data and training data sheets
	Exercise Books
	Train-the-Trainer Materials
Web-Based Training (WBT)	L2 interactive training (currently in Captivate and Flash format)
Distance Learning	Videoconferencing
	Telephone training

## 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 CBP and shall meet to the following requirements:

- Plan, prepare and facilitate 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 a CBP background investigation.

- Proposed personnel may be required to travel nation-wide to support requirements.
- Furnish, as required, training support personnel and services to assist CBP in developing and providing training to users of all automated systems and platforms supported by CBP, including: Microsoft applications; computer and web-based; and, interactive distance learning training.
- Follow the prescribed policies, life cycles, and standards of the CBP Systems Life Cycle (SLC) in developing, maintaining, or implementing information and technology projects and systems. The *System Life Cycle (SLC) Handbook* describes the official CBP policy that applies to all Information and Technology (IT) 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.
- 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

#### 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

#### DHS Management Directive 4010 Section 508 Program Management Office & Electronic and Information Technology Accessibility

- Version 2
- October 26, 2005
- Section 5.J Responsibilities
- Section 6.A Policies and Procedures
- (b)(2), (b)(7)(E)

#### 4. SPECIFIC TASKS

##### 4.1 Maintenance of Existing ACE and Legacy Training Materials

The Contractor shall maintain existing ACE and legacy system training materials. The current inventory of training materials eligible for maintenance includes:

**Table 4-1: Existing ACE and Legacy Training Materials**

Release	Course Name	Audience	Materials
<b>ACE Master Data and Enhanced Accounts (A1)</b>	A1 ESAR and Account Management Overview Web-based	CBP	Web-Based Training (WBT)
	A1 ESAR for Trade Community (A1)	Trade	WBT
	A1 ILT Resource Center	CBP	A1 simulations, A1 Course Content, A1 QRG
	A1 PGA Commodity Analyst	PGA	WBT
<b>ACE Initial Entry Summary Types (A2.2)</b>	A2.2 ACE Initial Entry Summary Types (A2.2) for PGA Commodity Analyst	PGA	WBT
	A2.2 ACE Initial Entry Summary Types for Census Commodity Analyst	PGA	WBT
	A2.2 Initial Entry Types (ESAR: Initial Entry Type)	CBP	WBT
<b>ACE Antidumping and Countervailing Duties and Additional Functionality (A2.3.1a)</b>	A2.3.1a Field ILT materials	CBP	Simulations, Student Guide
	A2.3.1a for PGAs	PGA	WBT
	A2.3.1a for Trade	Trade	WBT
	A2.3.1a HQ ILT materials	CBP	Simulations, student guide
	ACE ESAR/Antidumping and Countervailing Duties (AD/CVD)	CBP	WBT called A2.3.1a WBT for CBP
<b>ACE Periodic Payment (R3)</b>	R3 Periodic Payments R3	Trade	WBT
<b>e-Manifest: Trucks (R4)</b>	ACE Initial Login for Trade Account Owners	Trade	WBT
	R4 e-Manifest: Truck R4 for Trade	Trade	WBT
	R4 e-Manifesto: Camiones R4 -spanish version	Trade	WBT
	R4 ILT Training	CBP	R4 Exercises, R4 simulations
<b>Non-Release-Based ACE Training</b>	ACE Reports (Advanced)	PGA	WBT
	ACE Reports for CBP WBT	CBP	WBT
	ACE Reports for Trade	Trade	WBT
	Modifying ACE Reports ILT	CBP	
	ACE System Control Officers (SCO) User Provisioning	CBP	WBT
	Getting Started with ACE	PGA	WBT

	Multi-Modal Manifest and ESAR Enhancements for Trade (A2.1, A2.2)	Trade	WBT
<b>Legacy System Training (Non-ACE)</b>	Air AMS Trade Act 2002 ILT	CBP	Instructor Guide, Student Guide
	Sea Automated Manifest System	CBP	Instructor Guide, Student Guide, Train-the-Trainer Guide, User Guide

Maintenance tasks for existing training materials are performed on an as needed basis, as identified and directed by CBP. The number of training materials that will require maintenance during the period of performance of this contract will be determined by updates to ACE and legacy systems and will be prioritized by the CBP ACE Training Branch Chief.

#### 4.2 Development and Delivery of New ACE Curriculum

During the period of performance of this contract, CBP is scheduled to deploy ACE Rail and Sea Manifest (M1) capabilities. The Contractor shall provide courseware development supporting tasks and activities for this functionality, to include:

- Develop content specific to M1 functionality as it relates to business processes;
- Develop the M1 Final Training Plan that describes the content of the curriculum along with an updates assessment of the risks surrounding successful development and delivery of the training materials;
- Develop M1 User Documentation and Training Materials for CBP, the Trade Community and PGAs:
  - User Documentation and Training Material development as three phases:
    - M1 Draft User Documentation and Training Materials, delivered prior to the Test Readiness Review (TRR) milestone, which includes WBT storyboards;
    - M1 Approved User Documentation and Training Materials, delivered prior to the Production Readiness Review (PRR) milestone; this is a more mature version of the draft suitable for use during simulations and dry runs of the training curriculum and includes:
      - Materials as identified in Table 4-1.
      - Compliance with existing CBP evaluation processes and tools;
      - Incorporation of Lessons Learned identified during the Draft review;
    - M1 Final User Documentation and Training Materials delivered after the Operational Readiness Review (ORR) milestone and is the finalized version of the curriculum.
  - Develop M1 Draft Training Schedule and submit to CBP for review prior to PRR;
    - The M1 Final Training Schedule is delivered prior to ORR.
  - Deliver a dry run of the training sessions. Subject Matter Experts and Help Desk personnel shall participate in the dry run;
    - The Contractor shall distribute, collect, and submit the M1 Dry Run Participant Evaluation forms.

- Develop and deliver a Training Lessons Learned Document following submission and review of the Approved User Documentation and Training Materials.

See tables 5-1 and 5-2 for exact delivery dates for M1 materials.

#### 4.3 Account Services Desk

The Contractor shall provide personnel to staff and maintain the Account Services Desk, (ASD), which is operational twenty-four hours a day, seven days a week, three hundred and sixty-five days a year and supports approximately 14,600 clients. The Contractor shall maintain a user support network and provide virtual training (via telephone or internet) for the trade community and respond to questions, incidents, or customer issues. The Contractor ASD team shall address and respond to 86% of received incidents or requests and also facilitate collaboration between the ASD and the Technical Service Desk (TSD), to streamline costs and support processes.

- The Contractor ASD staff shall also provide virtual user-training services for the trade community (via telephone or internet) on ACE functionality, including account management functions such as crew, conveyance, and reports.
- The Contractor ASD staff shall provide virtual ACE user-training services (via telephone or internet) to the carrier community, including providing assistance in system login, navigation and password resets.
- In support of the move to mandatory e-Manifest, the contractor ASD staff shall participate in client outreach events and offer instruction in the use of the ACE Portal, including assisting in the user enrollment / activation process for Trade participants and ACE e-Manifest: Truck functionality.
- The Contractor shall identify key ASD team members to participate in ACE train-the-trainer sessions and provide that training to remaining members of the ASD.
- The Contractor shall provide reporting statistics on the Account Services Desk that align with the overall organizational structure and reporting needs, as defined by the Contracting Officer's Technical Representative (COTR).

The information below reflects six months of ASD Remedy ticket information.

E-Manifest/Direct Support to Clients	9,601
Account Access Management	2,666
Account Reactivations	865
SCAC/String 2 Errors	757
Transferred/Referred Tickets	470
ACE Portal/Carrier/Importer Creations	311
Total	14,670

#### 4.4 Client Representative Support

The Contractor shall staff a team of six Client Representatives who shall work alongside Government Client Representatives to provide the primary interface between the Trade and CBP in the use of automated commercial online systems. They facilitate initial communication, set

up, testing, troubleshoot systems problems, and assist Trade partners in using ACE Electronic Data Interchange (EDI) applications. They also:

- Guide the trade through the use of CBP automated systems, and serve as the contact person to assist in resolving systemic issues.
- Assist in explaining and marketing automated systems that pertain to the trade's business with CBP.
- Assist in providing training to individual trade participants or trade groups on the use of new and existing automated system modules.
- Assist CBP personnel with the research and analysis of complex automated system issues.
- Identify problems in CBP's programming, and communicate the particulars to the appropriate office.
- Define and recommend needed changes and/or enhancements to increase system efficiency.
- Monitor the trade participant's transmission of data to CBP, identify and review transmission errors, and help to resolve the issues.
- Participate in train-the-trainer sessions to provide training to remaining Client Representatives.

#### 4.5 Tactical Radio and Communication Training (TRaCT)

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: Technology Training and Technical Support's (TTSP) (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 (approximately 4000 users). Additionally, OFO is deploying more than 3,500 radios to their officers in the next ten months with a mandatory training requirement. TRaCT provides continual refresher training to over 2,000 DHS personnel yearly, supporting CBP and ICE. TRaCT has training requests and plans to train over 2,000 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 TRaCT tasks are defined below:

- The current class schedule for TRaCT in this award period is for 54 two-day ILT sessions for the year. The number of sessions may be revised as the total number of students to be trained is yet to be determined, but a limit of 24 students per class has been established. The current population of possible students is 6,000 with an expected student population of 1,300 students requiring this re-occurring training.
- A member of this group will be identified as a Subject Matter Expert and assist the Technology Training Center's Distributive Learning Team, (DLT). The DLT will be required to design, develop and deploy at least three virtual training sessions that will

posted on the Virtual Learning Center for later use by all CBP personnel. In the past it took 500 hours to develop and post a one-hour virtual training session.

#### 4.6 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.

#### 4.7 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.

#### 4.8 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:

- Develop a detailed functional design specification for the training program for CARGO. The functional design specification will document the requirements for the training program and be presented for approval prior to the start of development work.
- 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).

#### 4.9 Evaluation of Training Effectiveness

The Contractor shall assist CBP in utilizing 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.

#### 4.10 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 using the Government Printing Office (GPO).
- 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.

#### 4.11 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.

#### 4.12 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.

#### 4.13 Provide Automated Data Processing Technical Support

For each of the major computer application systems an 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 training data identification & creation, training environment business requirement definition, and training environment usage and scheduling

requirements. The support of the training environment is from a functional/business standpoint and does not require activities such as code/script generation.

#### 4.14 Anticipated Staffing Levels, Labor Categories, Travel, and Other Direct Costs (ODCs)

Table 4-2 details the staffing levels, labor categories, amount of travel and ODCs CBP anticipates for support during this period of performance.

**Table 4-2: Anticipated Staffing Levels, Labor Categories, Travel, and ODCs**

LABOR CATEGORY	# OF PEOPLE	TOTAL HOURS PER LABOR CATEGORY
Project Manager 1	1	2,000
Subject Matter Expert 3	8	16,000
Trainer 4	5	10,000
Programmer/Developer/Analyst/Architect 3	23	46,000
Programmer/Developer/Analyst/Architect 4	1	2,000
Programmer/Developer/Analyst/Architect 5	1	1,000
Administrative 4	1	2,000

TRAVEL DESCRIPTION	TOTAL TRIPS REQUIRED
Travel for Training & On-site Support (all ACE Releases as needed)	63
Travel for the Account Services Desk	10
Travel to support the Trade Support Network meetings	2
TRaCT Travel	54

ODC DESCRIPTION	# OF PEOPLE	# MONTHS
Costs for Digital Subscriber Line Service	21	10

## 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.

- 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.

**Table 5-1: ACE Release Estimated Milestone Schedule**

<b>Title</b>	<b>Date</b>
M1 Test Readiness Review (TRR)	October 28, 2010
M1 Production Readiness Review (PRR)	December 22, 2010
M1 Operational Readiness Review (ORR)	April 10, 2011

**Table 5-2: Documentation & Delivery Schedule**

<b>No.</b>	<b>Title</b>	<b>Due Date</b>
1	Updates to Legacy Training Materials	As Needed
2	Updates to ACE Training Materials	As Needed
3	M1 Final Training Plan	15 Calendar Days before the M1 TRR
4	M1 Draft User Documentation and Training Materials	9 Calendar Days before the M1 TRR
5	M1 Approved User Documentation and Training Materials	9 Calendar Days before the M1PRR
6	M1 Draft Training Schedule	15 Calendar Days before M1 PRR
7	M1 Final Training Schedule	9 Calendar Days before the M1 ORR
8	M1 Final User Documentation and Training Materials	7 Calendar Days after the M1 ORR
9	Training Lessons Learned Document	10/29/10
10	Contract Performance Reviews	Fourth Tuesday of each Month
11	Weekly Status Reports	Weekly, by Close of Business each Friday
12	Monthly ASD Status Reports	COB the First Week of Every Month
13	Integrated Baseline Review (IBR) documentation, after the delivery order, showing the products to be delivered, the budget by month, and the schedule for completion	Within 45 Days after task order award

### 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 have the knowledge and experience to administer 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.

The Contractor shall have experience using Dimensions software.

The Contractor shall be experienced in the use of Adobe Captivate, RoboHelp, MS Office Suite (including Word, PowerPoint, and Excel) and Flash applications as well as Learning Management Systems.

### Delivery of Training Methods

The Contractor shall be capable of delivering training using all of the following methodologies:

- Instructor-led classroom training
- Computer-based training (CBT)
- Web-based training (WBT)
- Interactive distance learning (IDL)
- Electronic online help
- Customer/user one-on-one and support documentation
- Other methods as appropriate

The Contractor shall conduct training at local sites within the Washington, DC metropolitan area, and field sites throughout the United States.

### Weekly Status Report

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 by close of business each Friday.

### Monthly Status Report

The Contractor shall use Earned Value Management (EVM) reporting techniques to support cost, schedule, and scope performance evaluation by CBP. The Contractor shall report monthly on project progress to CBP via a Contract Performance Review (CPR). The CPR report consists of five formats containing data for measuring contractors' cost and schedule performance. Format 1 provides data to measure cost and schedule performance by product-oriented Work Breakdown Structure (WBS) elements, the hardware, software, and services the Government is buying. Format 2 is not used at this time. Format 3 provides the budget baseline plan against which performance is measured. Format 4 shows the current and planned full time equivalent (FTE) personnel working on each task. The Format 5 is a narrative report prepared to supplement the other CPR formats and is used to highlight significant performance and other contract issues and topics. The Format 5 should be limited to one page and is supplemented with Variance Analysis Reports (VARs). VARs will contain analyses of significant cost and schedule variances that exceed management thresholds established by the CSPO for the program. CPR data is submitted by close of business the fourth Tuesday of the month.

The Contractor shall provide reporting statistics on the ASD on monthly basis. This report will be submitted by COB of the first week of the month and will cover the month prior.

### Integrated Baseline Review

At the Integrated Baseline Review, the project cost, schedule, and documentation will be baselined. The required documentation will be submitted to the COTR and will undergo an internal CBP review. If changes are needed in the documentation, detailed comments will be provided to the Contractor. The Contractor will be provided a timeline for re-submission of the documentation. The Contractor shall use track changes when providing revisions to any documents

### Acceptance Criteria

Deliverables provided by the Contractor are subject to review and approval by the COTR. The acceptance criteria for documentation include:

- Project documentation is complete and delivered by the dates listed in Table 5-2; and
- Appropriate collaboration has been accomplished to ensure an effective document and acceptance of the content by affected stakeholders.

## 6. GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION

The Government will furnish all software, data and equipment needed by the Contractor. 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.

## 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. Upon approval by the COTR, Account Services Desk (ASD) personnel (with the exception of the ASD lead) may work remotely from their homes.

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 requirements 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. All travel must be performed in accordance with the Federal Travel Regulation (FTR).

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 two weeks in advance and shall include the dates, locations, and estimated costs of the travel.

Travel for trainers and staff will be required in this task to perform duties. Travel includes an anticipated 75, (2 day) training trips, for CARGO and 54, (2 day) training trips for TRaCT, during the entire period of performance under this task order. Travel is based on trainers and area analyst who travel within the United States.

## 8. PERIOD OF PERFORMANCE

The period of performance for this task order will from September 21, 2010 to July 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 (WMG), BI Coordinator of any changes in access requirements for its personnel no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and reassignments including those to another contract. The Contractor/Project Manager is responsible for the completion and timely submission to the COTR of the CF-242 for all departing contract personnel. The Contractor shall provide OIT/WMG/BI Coordinator the following information on behalf of their contract personnel to telephone number (b) (6) or fax the below information to (b) (6)

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) (6) and FAX (b) (6)

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]

#### SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

(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 60 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.

(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 6.1.1, October 31, 2008) 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.

## 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.

## 10. SPECIAL CONSIDERATIONS

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

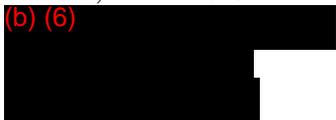
CBP, COTR

(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)

A large black rectangular redaction box covers the text in this block.

## ENTERPRISE ARCHITECTURE (EA) COMPLIANCE

The Offeror shall ensure that the design conforms to the DHS Homeland Security (HLS) and CBP EA, 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) version 2.0 and the CBP Architectural Modeling Standards for all models. Universal Modeling Language (UML2) may be used for infrastructure only. Data exchange formats and semantics shall be in conformance with the National Information Exchange Model (NIEM), version 2.0. Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

The contractor shall maintain close coordination with the CBP Enterprise Architecture Branch (EAB) and utilize the Central Enterprise Architecture Repository (CEAR), for capturing performance measures, business processes, application designs, technical infrastructure designs, and other related designs for the project. The contractor shall develop performance indicators and ensure appropriate mapping to the Performance Reference Model (PRM); develop business process flows and ensure appropriate mapping to CBP Lines of Business and Business Reference Model (BRM); develop application models capturing system components, subsystems, and information exchanges between system in development and other systems and ensure appropriate mapping of the system under development to Service Component Reference Model (SRM) and the Technical Reference Model (TRM); develop data models and data exchanges that align to the Data Reference Model (DRM) and develop models of technical infrastructure that will be used to support the systems under development.

All IT hardware and software shall comply with the DHS and CBP Technical Reference Models (TRM). 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.

Description information for 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 (DRM) and Enterprise Architecture Information Repository. Submittal shall be through the CBP Data Engineering Branch (DEB) and CBP Enterprise Architecture Branch (EAB).

All developed solutions shall be compliant with the HLS and CBP EA. Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

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

#### 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](mailto:accessibility@dhs.gov).