

**U.S. Customs and Border Protection  
Modernization Program**

**Task Order: Production Applications and  
Systems Support Maintenance**

**Statement of Work**

Version 1.6 Fiscal Year 2011

Publish date May 25, 2011

## Table of Changes

Revision Number	Date of Change	Section(s) Affected	Brief Description of Change	Change Made By	Organization
1.0	1/7/11	All	Initial Document	(b) (6)	CBP
1.1	3/30/11	3.9.1 and 4.2	Added ACE checkout procedures updated for M1 functionality; Added SWIT testing support; Removed Key Personnel	(b) (6)	
1.2	4/12/11	Various	Added goal of 90% discrete measurable tasks, added transition support language, rejected Key Personnel removal. added paragraph at beginning of CISS section and deleted Software Engineering and System Engineering Leadership and Governance scope sections.	(b) (6)	CBP
1.3,, 1.4, 1.5, 1.6	4/18/11 and 4/20/11 and 4/26/11 and 5/25/11	Various	Updated text as a result of negotiations and removal of CTOD language in section 3.11 once CTOD BOE was submitted	(b) (6) (b) (6)	AST

# Table of Contents

<b>1. Background and Introduction .....</b>	<b>6</b>
<b>2. Assumptions.....</b>	<b>6</b>
2.1 Dependencies.....	7
2.2 Desired Outcomes .....	7
2.3 Expectations of Performance.....	7
2.4 Key Milestones .....	8
<b>3. Scope of Work .....</b>	<b>8</b>
3.1 Foundation Program Management (FPM) (Program Level) .....	8
3.2 Facility Management (Program Level).....	8
3.3 Task Order Management (Task Order Level).....	8
3.3.1 Scope Management (Task Order Level).....	9
3.3.2 Schedule Management (Task Order Level) .....	9
3.3.3 Cost Management (Task Order Level).....	9
3.3.4 Resource Management (Task Order Level).....	10
3.3.5 Communications Management (Task Order Level).....	10
3.3.6 Risk Management (Task Order Level) .....	10
3.4 Team Management (Task Order Level).....	11
3.5 Productivity and Quality Improvement (Program Level) .....	12
3.6 PAM Quality Assurance Management (Production Delivery Level).....	12
3.7 Cargo IT Services and Support (CISS) (Program Level and Production Delivery Level by Subsection) .....	16
3.7.1 ACE Architecture and Integration Services (Program Level) .....	16
3.7.2 Systems Engineering Services (Program Level and Production Delivery Level by Subsection) .....	19
3.7.2.1 Requirements Management (Program Level) .....	20
3.7.2.2 Systems Engineering Support Activities (Production Delivery Level) .....	21
3.7.3 Performance Engineering (Production Delivery Level) .....	21
3.7.4 Security Services (Program Level and Production Delivery Level by Subsection) .....	22
3.7.4.1 Security Activities (Program Level) .....	22
3.7.4.2 Security Support Activities (Production Delivery Level) .....	23
3.7.5 Configuration Management (Program Level and Production Delivery Level by Subsection) .....	24
3.7.5.1 CM Support (Program Level) .....	24
3.7.5.2 CM Support (Production Delivery Level).....	25
3.7.6 Engineering and Development Tools Administration (Program Level).....	25
3.7.6.1 Engineering and Development Tools Administration Support Activities (Program Level) .....	26

3.8	ACE Operations & Maintenance (O&M) (Program Level and Production Delivery Level by Subsection) .....	26
3.8.1	ACE Level 2 Application Support (ACE Application Analysis and Support) (Production Delivery Level) .....	26
3.8.1.1	Level 2 Application Support Activities (Production Delivery Level) .....	27
3.8.2	Electronic Data Interchange (EDI) Support (Program Level and Production Delivery Level by Subsection) .....	28
3.8.2.1	EDI Support (Program Level) .....	28
3.8.2.2	EDI Support (Production Delivery Level) .....	28
3.9	ACE Production Application Maintenance (PAM) Services (Program Level and Production Delivery Level by Subsection) .....	29
3.9.1	PAM Activities (Program Level) .....	30
3.9.1.1	Delivery Integration (Program Level) .....	30
3.9.1.2	Support working groups and IPT (Program Level) .....	30
3.9.1.3	Problem investigation (Program Level) .....	30
3.9.2	PAM Activities (Production Delivery Level) .....	30
3.9.2.1	Problem investigation (Production Delivery Level) .....	30
3.9.2.2	Immediate Response (Production Delivery Level) .....	31
3.9.2.3	Level 3 (L3) Application Support (Production Delivery Level) .....	31
3.9.2.4	PTR Support (Production Delivery Level) .....	31
3.9.2.5	CR Support (Production Delivery Level) .....	33
3.9.2.6	COTS Upgrades (Production Delivery Level) .....	35
3.9.2.7	SAT Support (Production Delivery Level) .....	35
3.9.2.8	Planning and Coordinating (Production Delivery Level) .....	36
3.10	ROM Effort and Analysis .....	36
3.11	Communications, Training, Outcomes, and Deployment (CTOD) (Program Level) .....	37
<b>4.</b>	<b>Project Staffing</b> .....	<b>37</b>
4.1	ACE Support Team Resources .....	37
4.2	Key Personnel .....	38
4.3	Transition Support .....	39
<b>5.</b>	<b>Acceptance Criteria</b> .....	<b>39</b>
<b>6.</b>	<b>Accessibility Requirements (Section 508 Compliance)</b> .....	<b>39</b>
<b>7.</b>	<b>Deliverables and Delivery Schedule</b> .....	<b>41</b>
<b>8.</b>	<b>Contractor-Furnished Materials &amp; Other Direct Costs</b> .....	<b>41</b>
8.1	Escrow .....	41
8.2	Tools .....	41
<b>9.</b>	<b>Travel</b> .....	<b>42</b>
<b>10.</b>	<b>Period of Performance</b> .....	<b>42</b>
<b>11.</b>	<b>Place of Performance</b> .....	<b>42</b>

<b>12. Security</b>	<b>42</b>
12.1 Security Review and Reporting	42
12.2 Interconnection Security Agreements	43
12.3 Security Requirements for Unclassified Information Technology Resources	43
12.4 Contractor Employee Access	44
12.5 Information Security (ISO) Compliance	45
12.6 Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information	45
<b>13. Engineering Platforms</b>	<b>45</b>
<b>14. Enterprise Architecture Compliance</b>	<b>46</b>
<b>15. Transition Plan</b>	<b>48</b>
<b>16. Program Management Tool for Reporting</b>	<b>49</b>
<b>17. Government Project Leadership Contacts</b>	<b>50</b>

## List of Tables

<b>Table 2-1 Assumptions</b>	<b>6</b>
<b>Table 2-2 Dependencies</b>	<b>7</b>
<b>Table 3-1 PAM Performance Measures</b>	<b>13</b>
<b>Table A-1 Required Artifacts</b>	<b>51</b>

# 1. Background and Introduction

U.S. Customs and Border Protection (CBP) is modernizing its business processes, Information Technology (IT) systems, and infrastructure to provide functionality needed to support its missions of trade facilitation, trade compliance and trade enforcement. This modernization involves applying the CBP Enterprise Life Cycle Methodology (ELCM) to integrate multiple projects and other ongoing CBP operations into a comprehensive and integrated CBP Modernization Program.

A key Modernization effort supporting CBP missions is the development of the Automated Commercial Environment (ACE) system, which will replace and/or supplement the current functionality of the Automated Commercial System (ACS) and other related CBP systems.

While the ACE system is currently production operational, not all functionality has been delivered. During this period of performance, the remaining two major development releases are scheduled to be completed. This Statement of Work (SOW) supports the production application needs as well as the architectural, engineering, configuration management, and security services needed to support the development efforts.

The current ACE Technical Architecture incorporates best practice techniques to provide a framework for delivering a secure, scalable, highly available, and extensible architecture. A “defense-in-depth” strategy spans the n-tier architecture to support secure and authorized access to data for both the trade and CBP. The architecture is based on the use of open standards and logical tiers grouping common functionality and services. The remainder of the Modernization technology in the data center uses existing CBP technologies. Additional new software technologies introduced include industry leading tools for large-scale data transformations and data reporting, security management products, and search engine software for indexing.

# 2. Assumptions

This section provides the identified assumptions related to the SOW.

**Table 2-1 Assumptions**

#	Assumption	Area
1.	All outputs will meet established CBP standards, policies, processes, and procedures.	All
2.	CBP will provide access to Subject Matter Experts (SMEs) and Business Process Owners (BPOs) empowered to recommend/approve business process, organizational, and legal/policy decisions.	CBP
3.	CBP will provide support to conduct clearances for the personnel performing on the task order.	CBP
4.	CBP will identify points of contact, and will assist in gaining access to SMEs for all systems related to the scope of the project.	CBP

#	Assumption	Area
5.	CBP will provide required access to CBP system documentation, plans, and status of ongoing and future development efforts, and information necessary to develop requirements and specifications for proposed changes to CBP systems, as applicable.	CBP
6.	Support will be provided to all ACE environments independent of location.	All
7.	The Contractor shall enforce standard structured software development engineering practices as defined in American National Standards Institute (ANSI)/Institute of Electrical and Electronics Engineers (IEEE). Special attention will be paid to the enforcement of documented design and coding standards and SLC document traceability to demonstrate that all requirements have been designed, incorporated into code, and tested.	Contractor
8.	All work will adhere to DHS Acquisition Directive 102.01 (DHS Systems Engineering Lifecycle (SELG))	All

## 2.1 Dependencies

The following dependencies are associated with the approach and project team structure for accomplishing the activities outlined in this SOW.

**Table 2-2 Dependencies**

Owner	Dependencies
CBP	CBP will provide resources to identify (e.g., via System Acceptance Testing (SAT)) and prioritize all Product Trouble Reports (PTRs) and Change Requests (CRs).
CBP	Enterprise Data Management and Engineering (EDME) and Enterprise Network and Technology Services (ENTS) will communicate all infrastructure activities with the Cargo System Program Office (CSPO) and the Contractor in advance of implementation planning and shall embed these activities within the ACE Integrated Master Schedule (IMS).
CBP	EDME will provide production change management for CBP and the Contractor.

## 2.2 Desired Outcomes

Outcome 1: Anticipate and provide the support needed to meet ACE Cargo Program release milestones while achieving expected availability, quality, security, reliability, maintainability, interoperability, flexibility, and extensibility across all areas of ACE.

Outcome 2: Achieve availability and performance levels for the production and support environments so as not to impact the ACE schedule or end users.

## 2.3 Expectations of Performance

The Contractor shall:

- a) Plan and forecast Contractor requirements, opportunities, dependencies, and constraints.

- b) Regularly communicate with CSPO Division managers, including early and candid notification on risks and issues.
- c) Pro-actively define and document for Government acceptance, risk mitigation activities and issue resolution plans.
- d) Identify the sequencing of the key processes, interrelationship, and dependencies on other program activities or approval processes and provide close and effective coordination across all Contractor collaboration points.
- e) Submit deliverables and work products on schedule that receive Government approval with no rework required.
- f) Provide products and perform activities that are planned, developed, and implemented in accordance with applicable laws, regulations, policies, and processes.
- g) Coordinate in advance with CSPO on all plans or proposals for interaction with ACE stakeholders including EDME and ENTS.
- h) The Contractor's Task Proposal(s) and performance there under shall comply with all provisions of the base contract.
- i) The Contractor shall actively support the involvement and mentoring of CBP personnel or designee in any and all activities it undertakes within the scope of performing its mission. Should such an involvement lead to the increase in scope of said activities, the Government, solely at its discretion, will review and authorize additional scope for the increase.

## **2.4 Key Milestones**

All release milestones are recorded in the ACE Integrated Master Schedule (IMS).

## **3. Scope of Work**

### **3.1 Foundation Program Management (FPM) (Program Level)**

General FPM activities are detailed in Section 2.1 Foundation Program Management (FPM) of the ACE Development Support Reference Document (DSRD).

Additionally, the Contractor shall collaborate with the Government to achieve the goal of 90% discrete measurable tasks.

### **3.2 Facility Management (Program Level)**

General Facility Management activities are detailed in Section 2.2 Facility Management of the ACE DSRD.

### **3.3 Task Order Management (Task Order Level)**

Focuses on the overall scope, cost/budget, quality assurance, resources, communications, risk, and deliverable management for all services addressed in this task order (TO). Emphasis will be

placed on providing flexible services required to support a dynamic production application and developing system, within the cost constraints of this contract.

### **3.3.1 Scope Management (Task Order Level)**

The Contractor shall perform scope management for the task order to include:

- a) Maintain contractual scope for the task order.
- b) Provide a complete and comprehensive scope assessment for application changes (whether in the form of a Great Idea Form (GIF), PTR, or CR). This assessment shall include efforts required to successfully implement the change without impacting the integrity of any potentially affected system and/or application. This assessment shall also include documentation update efforts.

### **3.3.2 Schedule Management (Task Order Level)**

All TO Production (PROD) activities shall be planned and scheduled. The Contractor shall:

- a) Support the Government in organizing, planning, and scheduling future production and application deployment implementations.
- b) Include the project schedule for all TO PROD activities within the ACE IMS.
- c) Perform schedule analysis of the ACE IMS to identify scheduling risks.
- d) Provide data to support the Government's CSPO Program Management Reviews (PMRs).

### **3.3.3 Cost Management (Task Order Level)**

The Contractor shall receive Government approval before performing overtime work (more than 40 hours overtime a month per Full Time Employee (FTE)). The Contractor is expected to effectively manage to this period of performance cost constraint, and shall perform the following activities:

- a) Ongoing resource planning.
- b) Cost estimating.
- c) Ongoing and additional funding, budget, and expenditure analysis to support TO cost control.
- d) Leadership of activities related to the monthly cost performance monitoring cycle, to include conducting monthly Internal Cost Review meetings as well as coordinating completion of Estimates to Complete (ETC) and Variance Analysis Reports (VARs) for control accounts throughout the TO.
- e) Monitoring, tracking, and analysis of project labor and expenditures.
- f) Establishment and maintenance of labor and expense charging mechanisms for Contractor staff (charge codes, work packages).
- g) Subcontractor Invoice Reviews.
- h) Monthly Contract Performance Review (CPR) and coordination.
- i) Coordinating Contracting Officer's Technical Representative (COTR) approval for required non-labor expenditures, such as non-local travel and other direct costs.

### **3.3.4 Resource Management (Task Order Level)**

The Contractor shall provide resource management support for this TO which involves a significant amount of planned and unplanned activities which require service teams comprised of the appropriate technical, process, management, and organizational change skills. The Contractor shall stay vigilant in managing the team resource needs to maintain a flexible service offering by managing the effort to:

- a) Perform timely resource and/or assignment changes to avoid schedule delays, disruptions, conflicts or create unexpected problems.
- b) Perform timely identification of resourcing risks associated with assigned work so that they may be properly mitigated or addressed.
- c) Supply inputs to enable the basic business controls that focus on authorizing resources to work on the project, skill code analysis, and provide exit notifications to the Contractor's staffing team.

### **3.3.5 Communications Management (Task Order Level)**

The Contractor shall communicate regular status items for the TO to the COTR as follows:

- a) Consolidate Team Lead Weekly Status Reports to include the following:
  - Updated task Work Breakdown Structures (as required)
  - Updated project schedule
  - List of current tasks and their status, including dependencies
  - Activities completed
  - CR Status
  - Accomplishments for the prior week
  - Planned activities for the next week
  - Summary-level status of Outstanding risks/issues/concerns
- b) PTR Summary (Production Application Maintenance (PAM) Production only) categorized by:
  - High Risk PTRs and PTR Oversight assessment, monthly trend analysis
  - Emergency PTRs
  - Total Number of PTR sorted by categories defined by the Government. i.e., sort the PTRs by Business Area (Account, Portal, EIS, Transactions)
  - PTRs to be categorized
  - PTRs planned
- c) Support the Government's monthly CSPO PMRs and CPRs

### **3.3.6 Risk Management (Task Order Level)**

The effective management of risks and issues is critical to attaining the financial, schedule, and technical objectives of the TO. Risks and issues are addressed through a structured approach applied at the TO level through out the life cycle of the program. The Contractor shall execute Risk Management for the TO by performing the following activities:

- a) The Contractor shall coordinate collection of risk and issue assessments, responses, and status updates from affected stakeholders, as part of their risk management and

mitigation activities and verify that proper recording and status updates are applied in the Active Risk Manager (ARM) tool.

- b) The Contractor shall consider the cost and schedule impact if risks/issues are realized.
- c) The Contractor shall include risk/issue status information in monthly CPR and PMR presentations.

### **Outputs in Addition to Required System Life Cycle (SLC)/Systems Engineering Life Cycle (SELC) Outputs**

- TO PROD schedule (of all activities) to be incorporated into the ACE IMS
- Data updates for input into the Monthly CSPO PMR and CPR
- Consolidated Team Lead Status Report (weekly)

## **3.4 Team Management (Task Order Level)**

The Contractor shall perform team management to maintain the integrity of the application while containing costs and minimizing risk. Therefore, the Contractor shall perform team-level Scope Management, Schedule Management, Cost/Budget Management (e.g., Cost Account Management), Quality Assurance, Resource Management, Communications Management, Risk Management and Deliverables/Contract Output Management in accordance with CBP guidelines.

As part of team management duties, the Contractor shall:

- a) Prioritize team activities, in collaboration with the Government, and verify that the teams are following the ACE Program and CSPO change management processes.
- b) Coordinate collection of risk and issue assessments, responses, and status updates from affected stakeholders, as part of their risk management and mitigation activities and verify proper recording and status updates are applied in the ARM tool.
- c) Consider the cost and schedule impact if risks/issues are realized.
- d) Provide to the TO Management, a weekly status to include the following:
  - Updated project work planning
  - List of current tasks and their status, including dependencies
  - Activities completed
  - Accomplishments for the prior week
  - Planned activities for the next week
  - Outstanding issues/concerns

Team managers shall perform activities related to the monthly cost performance monitoring cycle, to include participating in monthly Internal Cost Review meetings as well as completing ETCs and VARs for control accounts throughout the TO.

The activities performed and services provided to support the production ACE application are highly dynamic. As such, the Government will provide guidance in determining team priorities, with emergency problem resolution always taking precedence. Therefore, the team management support for PAM includes the following services in support of the Government's efforts to determine effective priorities and planning:

- a) The Contractor shall perform only Government-authorized work and shall follow the appropriate CBP processes to obtain authorization on any production application changes.

- b) Non-corrective and non-emergency maintenance services, as required at the direction of the Government, shall be planned and scheduled. The Contractor shall manage these scheduled activities and provide risk, issue, and corrective action recommendations as soon as potential slippages become known. The Contractor shall also include total cost of corrective action recommendations as well as impacts to other current and future planned work.
- c) The Contractor shall support the Government in organizing, planning, and scheduling future production environment and application deployment implementations.
- d) The Contractor shall provide a project schedule, with dependencies and resources required, to the Government. The schedule will be updated and reviewed weekly with the Government.

### **3.5 Productivity and Quality Improvement (Program Level)**

The Contractor shall implement Government-approved Delivery Excellence recommendations intended to support the remaining ACE development projects and ongoing PAM quality and productivity increase goals per the performance measures. This scope will be funded and managed only as needed by Government-approved CR.

### **3.6 PAM Quality Assurance Management (Production Delivery Level)**

Quality Assurance (QA) will be performed in accordance to the ACE Quality Management Plan, 02-eCP-2611. The Contractor shall provide assessments of all activities performed within this task order to measure the degree of compliance of all policies, processes, and procedures that affect the quality of new delivered functionality and ongoing maintenance work. The results of these assessments will feed back into the ongoing improvement efforts performed within the architecture, system engineering, and software engineering functions.

- a) The Contractor shall perform the following activities to monitor PAM compliance:
  - Verify progress and completion of Corrective and Preventive Actions (CAPAs).
  - Verify that Software Integration and Test (SWIT) Testing occurred and is completed.
  - Participate in approximately 50-75% of PAM Peer Reviews and Inspections to verify that the review and inspection process is followed and that the review criteria have been applied.
  - Verify that appropriate inspections have occurred and action items are closed for CRs and PTRs prior to their implementation in production.
  - Verify the process for PTR write-ups is followed by participating at PAM PTR Review Board.
  - Perform internal process audits (schedule, perform, report) and report findings directly to the Government. Findings will also be provided to the architecture, system engineering, and software engineering teams to determine if process/procedure update recommendations should be developed.

- Conduct and document Lessons Learned during agreed to milestones in the delivery schedule and make available for all Contractor and Government ACE development/maintenance personnel.
- Monitor closure of lessons-learned action items and track the update of processes, procedures, standards, etc as needed.
- Recommend process improvements as the result of day-to day interactions, the audits, trends, and reviews and inspections.

**Outputs in Addition to Required SLC/SELC Outputs**

- List and schedule of all audits to be conducted by the QA team.
- Audit assessment findings.
- Lessons Learned documentation with demonstration that all relevant processes, procedures, standards, etc. have been updated to reflect learned lessons.
- Corrective and Preventive actions status and reports
  - b) Measurements:
    - Develop, review, and submit the Performance Measurement Report for PAM Performance Measure Results defined below.
      - 1) The Contractor shall submit a proposal within 10 days of Task Order Period of Performance start date of January 30, 2010 (POP start date) that describes how to flag rework PTRs and CRs within Dimensions. Solution must be implemented by the Contractor within 30 days of POP start date.
      - 2) The Contractor shall submit a proposal within 10 days of POP start date that describes how to measure PTR and CR removals from a planned drop without negatively impacting the schedule.
    - Using the Performance Measurements, refine activities including process compliance, peer review process oversight, lessons learned collection and reporting, metrics framework collection, analysis, trending, and reporting.

**Table 3-1 PAM Performance Measures**

Desired Outcomes	Required Services	Performance Standard	Acceptable Quality Level (AQL)	Monitoring Method	Measurement Category	Data Source
Complete scheduled Production Application Maintenance work on time	ACE Production Application Maintenance	Maintain Government and Contractor agreed-upon, SWIT complete dates for CRs and PTRs (unless dates are changed by Government and/or impacted by EDME/ENTS infrastructure changes).	95% of the time (calculated quarterly)	Quarterly Measurement (Reported Monthly)	Schedule	ACE PAM work plan
Achieve a modular approach to release packaging to	ACE Production Application Maintenance	For scheduled PAM releases, the Contractor shall provide the Government the	80% of the time (calculated quarterly)	Quarterly Measurement (Reported Monthly)	Package Flexibility	ACE PAM work plan

Desired Outcomes	Required Services	Performance Standard	Acceptable Quality Level (AQL)	Monitoring Method	Measurement Category	Data Source
allow flexibility for individual PTRs and CRs to be removed without negatively impacting the planned drop schedule.		ability to remove individual CRs or PTRs within two weeks of the drop.	See 3.6.b.2			
Minimize or eliminate rework and reduce defects delivered to production.	ACE Production Application Maintenance	Percent of CRs requiring rework during SAT	15% of all CRs	Quarterly Measurement (Reported Monthly)	Quality	Dimensions
Minimize or eliminate rework and reduce defects delivered to production.	ACE Production Application Maintenance	Percent of PTRs requiring rework during SAT	15% of all PTRs	Quarterly Measurement (Reported Monthly)	Quality	Dimensions
Improve the estimating accuracy for CRs and PTRs	ACE Production Application Maintenance	Actual-to-plan hours estimating ratio	0.8 to 1.2.	Reported Monthly  For CRs, the monitoring method will be WBS for Government-designated CRs, for all other CRs: Dimensions work orders.  For PTRs, estimates are tracked in the work plan, and actuals pulled from Dimensions work orders once work is complete	Estimating Accuracy	Dimensions, WBS for Government-designated CRs
Provide efficient turnaround on requested ROMs used for budgeting and estimating purposes.	ACE Production Application Maintenance	Percentage of time that Rough Order of Magnitude Hours Estimates (ROMs) for PTRs, GIFs, and CRs are completed within 10 business days of CBP	95% of the time	Quarterly Measurement (Reported Monthly)	ResponsivenessQuality	GIF FormsRemedy, RCA Data

Desired Outcomes	Required Services	Performance Standard	Acceptable Quality Level (AQL)	Monitoring Method	Measurement Category	Data Source
Provide efficient turnaround on requested ROMs used for budgeting and estimating purposes	ACE Production Application Maintenance	Percentage of time that Funding Estimates for PTRs are completed within 30 business days of CBP request.	75% of the time	Quarterly Measurement (Reported Monthly)	Responsiveness	PTR Form
Provide efficient turnaround on requested ROMs used for budgeting and estimating purposes	ACE Production Application Maintenance	Percentage of time that Funding Estimates for CRs are completed within 45 business days of CBP request	75% of the time	Quarterly Measurement (Reported Monthly)	Responsiveness	CR Form GIF Forms
Improve ACE Application Sev 1 and Sev 2 resolution times*.	ACE Production Application Maintenance	<p>- ACE O&amp;M Sev 1 ACE Application tickets must be resolved within 12 hours. The remaining Sev 1 tickets must be resolved within 24 hours.</p> <p>- ACE O&amp;M Sev 2 ACE Application tickets must be resolved within 24 hours. The remaining Sev 2 tickets must be resolved within 72 hours.</p> <p>- ACE O&amp;M Sev 3 ACE Application tickets must be resolved within 1 month</p>	<p>- 70% or greater of ACE O&amp;M Sev 1 ACE Application tickets must be resolved within 12 hours. The remaining Sev 1 tickets must be resolved within 24 hours.</p> <p>- 50% or greater of ACE O&amp;M Sev 2 ACE Application tickets must be resolved within 24 hours. The remaining Sev 2 tickets must be resolved within 72 hours.</p> <p>- 50% or greater of ACE O&amp;M Sev 3 ACE Application tickets must be resolved within 1 month.</p>	Monthly Measurement	Quality Responsiveness	Remedy

\* NOTE: Resolution of Sev 1 and Sev 2 Trouble Tickets defining Operations-related problems would include an acceptable work-around being in place to support ACE functionality. Trouble Ticket closure will extend beyond 'Resolution' time to verify that appropriate corrective and preventive actions are documented in the Trouble Ticket for appropriate closure.

### **Outputs in Addition to Required SLC/SELC Outputs**

- PAM Performance Measure Results as described in Table 3-1.

## **3.7 Cargo IT Services and Support (CISS) (Program Level and Production Delivery Level by Subsection)**

### **3.7.1 ACE Architecture and Integration Services (Program Level)**

The ACE application is hosted on an infrastructure that is primarily designed and operated by the OIT EDME organization. As of 2009, the infrastructure supporting ACE is a dedicated infrastructure. It is expected that over time the ACE infrastructure will be consolidated with other CBP OIT and DHS infrastructures and that ultimately ACE will be hosted entirely on a common enterprise infrastructure. While the OIT EDME organization has full responsibility for the infrastructure architecture and design (dedicated components as well as common enterprise infrastructure components) this architecture task has the responsibility to provide the overall coordination of the ACE application and *dedicated* ACE infrastructure architectures to facilitate continued enterprise architecture alignment and successful PADR and SLC/SELC milestone reviews.

As such, the described ACE Architecture and Integration services by necessity are provided at a program level coordinating across the M1 development completion and ACE PAM projects and activities, for the Contractor to achieve and maintain:.

- An ACE architecture that supports the implementation of the system in a manner that can gracefully accept unexpected workloads and be capable of increasing workload capacity through vertical or horizontal scaling of the underlying infrastructure.
  - A flexible ACE architecture that will facilitate the extension of existing capabilities as well as the addition of new capabilities without requiring significant changes to the existing architecture components.
  - An ACE architecture based on open standards and protocols to facilitate interoperability of the system.
  - ACE architecture that supports the implementation of the system in a modular manner, allowing for the separation of functional layers and packages and minimization of interdependencies of components in the system.
- a) Maintenance of ACE Architecture Artifacts in accordance with the release-level tailored System Life Cycle (SLC)/ System Engineering Life Cycle (SELC) and the ACE release schedules. Artifacts shall include:
- The ACE High-Level Architecture Description and Diagram (formerly referred to as the ACE Conceptual Architecture) which provides a visual and narrative summary of the ACE architecture.

- The ACE Operational Model (Logical) which defines the operational technical requirements needed for the ACE system to operate in production (EDME will use the logical operational model to develop and maintain the ACE physical infrastructure).
  - The ACE High-Level Data Model (formerly referred to as the ACE Data Conceptual Model) used for Architecture Alignment Assessment (AAA) reviews and by the Department of Homeland Security (DHS) Enterprise Data Management Office (EDMO).
  - The ACE Database Data Management Plan, a SELC-required artifact.
  - The ACE Data Dictionary to include a descriptive definition for all data elements.
- b) Integration Services to provide Technical Integration Leadership and Governance across ACE delivery and maintenance projects:
- The Contractor shall maintain and enforce currently documented ACE architecture and data and software design principles, standards and guidelines.
  - The Contractor shall provide leadership and decision authority for all internal (to the Contractor) technical change management decisions.
  - The Contractor shall participate in program change management activities.
  - The Contractor shall actively monitor development projects to quickly identify release specific and integration related technical issues and lead ongoing forums to facilitate the resolution of these issue across the ACE teams to avoid escalation as Program-level risks/issues. Issues shall be documented and furnished to the Government in the TO PROD weekly status report.
  - The Contractor shall participate in routine forums to monitor production operations to identify key operational and technical integration issues and facilitate the identification of resolutions for these issues. Risks and issues shall be documented and furnished to the Government in the TO PROD weekly status report.
  - The Contractor shall provide architecture/design leadership direction and guidance to the development projects by:
    - 1) Providing senior technical expertise in resolving complex problems identified during the release development testing stage.
    - 2) Providing insight into the expectations of the AAA reviews, DHS Program Assessment and Design Reviews (PADR), and SLC/SELC milestone reviews and how to effectively prepare for these reviews.
    - 3) Reviewing key development project work products, during the timeframe described in the release project schedules, to assess:
      - Technical viability of release design
      - Alignment of the release design to the ACE architecture and ACE design principles.
      - Alignment with the enterprise architecture and ability to achieve CBP mission objectives.

Report any risks or issues at the TO Production status report.
  - The Contractor shall adhere to DHS Acquisition Directive 102.01 (DHS SELC)

- The Contractor shall serve as the communication point of contact for notifying ACE development and maintenance projects of changes to existing CBP and DHS enterprise technical goals, requirements, guidelines, standards (including DHS PADR and Office of Information and Technology (OIT) Architecture Alignment Assessment (AAA) process and evaluation criteria) that affect cost, schedule or quality. At Government direction, the Contractor shall also assist ACE teams to determine the most effective method of complying with changes that results in impact to cost, schedule and quality, and communicate change impacts to the Government in the weekly status report prior to implementing any changes.
- c) Provide inputs to the CBP enterprise architecture Technical Reference Model (TRM).
- The Contractor shall prepare and monitor technology insertion requests and Commercial off the Shelf (COTS) version upgrade requests for new or revised ACE components to update the standards profile in the CBP TRM. Only engineering and software development tools used to design and construct ACE application are the responsibility of this task; the OIT EDME organization is responsible for ACE infrastructure technology insertion.
  - Support the preparation of all trade studies to:
    - 1) Identify candidate technologies and standards to be proposed.
    - 2) Ensure the trade study accuracy and completeness.
    - 3) Ensure integration within the existing technology and process framework is achieved.
- d) The Contractor shall maintain a two-year technology and standards outlook for engineering and software development tools used to design and construct the ACE application. The OIT EDME organization is responsible for the ACE infrastructure technology outlook. Services include:
- Establishing and maintaining the ACE COTS Roadmap with at least an eighteen month outlook.
  - Tracking the schedules of new versions and sunset dates of existing products and new packages that may be incorporated in the future.
  - Documenting how existing COTS products may evolve over time, and where those evolutions may lead to overlapping functionality that could permit the elimination or consolidation of products.
  - Providing inputs to OIT EDME organization to identify future product features, technology, and standards that are required to support or minimize the costs to develop the ACE application.
- e) Sponsor and lead initiatives to resolve ACE architecture or design issues/risks or needs to meet upcoming functional or business requirements. This includes activities such as:
- Developing white paper solution concepts
  - Performing proof of concept implementations
  - Performing trade studies
  - Leading pilot efforts

- f) The Contractor shall support on-going CSPO activities as directed by the Government, including:
- Responding to ad hoc data and information requests.
  - Analyzing high-priority topics and issues.
  - Preparing briefings and reports.
  - Providing inputs to the ACE Transition Plan.
  - Supporting CSPO in the execution of CBP and DHS transitional strategies and architecture alignment and assessment activities.
  - The Contractor shall participate in enterprise working groups as directed by CSPO.

#### **Outputs in Addition to Required SLC/SELC Outputs**

- ACE High-Level Architecture Description and Diagram.
- ACE Operational Model (Logical).
- ACE High-Level Data Model.
- ACE Data Dictionary.
- ACE COTS Roadmap (for engineering and software development tools used to design and construct the ACE application).
- Inputs to the EDME COTS Roadmap (as required).
- Technology Insertion Requests (as required).
- Trade Studies (as required).
- Prototypes and proof of concepts.
- Briefings and Reports (as required).
- ACE Database Data Management Plan.
- Weekly status report to TO Management.

### **3.7.2 Systems Engineering Leadership and Governance Services (Program Level and Production Delivery Level by Subsection)**

The systems engineering leadership and governance services task maintains the complete set of ACE functional and technical requirements to reflect any new or modified business processes and technical solutions. This task also provides technical leadership and governance for all ACE Systems Engineering activities to ensure consistency, integrity, and reliability of the resulting Systems Engineering products. Systems Engineering activity is provided in four key areas:

- M1 ACE Business Process Hierarchy
- M1 ACE functional system architecture, defined in the release System Segment Design Description (SSDD)
- M1 ACE requirements management
- M1 ACE systems engineering practices, procedures, and tools

#### **3.7.2.1 Systems Engineering Leadership and Governance (Program Level)**

The Contractor shall perform the following Systems Engineering services in support of the ACE Business and Functional Architecture:

- a) Participate in technical and program change management activities.
- b) Work with the CBP business representatives to maintain and update the ACE Business Process Hierarchy that aligns the high level ACE Business Processes with the CBP
- c) Support Enterprise Architecture Line of Business Model at the direction of the ACE Executive Business Owner.
- d) Support on-going CSPO System Engineering activities as directed by the Government, including:
  - Responding to ad hoc data and information requests
  - Analyzing high-priority topics and issues
  - Preparing briefings and reports
- d) Maintain and enforce currently documented ACE system engineering principles, standards, and guidelines.

#### **Outputs in Addition to Required SLC/SELC Outputs**

- Business Process Hierarchy updates (at gate reviews).
- Government ad hoc request responses.

#### **3.7.2.2 Requirements Management (Program Level)**

The objective of the Requirements Management service is to manage the formal Configuration Management (CM) requirements baseline. Management of this baseline is performed using a CM tool which stores all baselined requirements or reference links to artifacts describing lower-level requirements.

To achieve this objective the Contractor shall perform the following services:

- a) Perform comparative analysis of updated baselines to the previous baselined version to verify that:
  - All requirements changes are properly accounted for in change requests.
  - Requirements traceability between the requirement artifacts has been properly provided by the release teams.
  - Correct syntax, format, and numbering are maintained.
- b) Perform Requirements Administration:
  - The Contractor shall perform the physical updates to the Requirements Management Tool (e.g. Dimensions RM) data based upon the data received by the release and PAM teams. Updates are expected to be performed for all approved CRs necessitating data changes recorded in the Requirements Management Tool (i.e. requirement changes, traceability changes, etc.).
  - The Contractor shall store and maintain the working and baselined versions of all requirement sets in a version controlled automated repository.
  - The Contractor shall maintain the ACE infrastructure requirements within the ACE requirements management tool.

- The Contractor shall generate ad hoc requirement reports at the request of the Government. The Contractor shall also recommend content for reports that would provide the Government with insight into the overall requirements effort, help the Government manage the overall requirements effort and provide root cause/trend analysis.

#### **Outputs in Addition to Required SLC/SELC Outputs**

- Ad hoc reports per Government request
- Requirements baselines (at gate reviews)

### **3.7.3 Software Engineering Leadership and Governance Services (Program Level)**

The Software Engineering task provides technical leadership and governance across all of the ACE development projects to ensure consistency, integrity, and maintainability of the delivered software through enforced software engineering practices, procedures, and tools.

The Contractor shall perform the following activities to maintain and enforce software engineering industry standards, principles, practices, procedures, and effective integrated use of software engineering tools across all the ACE development and maintenance projects to improve the quality of code delivered:

- a) The Contractor shall participate in technical and program change management activities.
- b) The Contractor shall develop processes to imbed static code analysis of all developed, or modified, source code, as a required software development activity.

#### **Outputs in Addition to Required SLC/SELC Outputs**

- Software development process defining use and enforcement of static code analysis.
- Provide updated Engineering policies, standards, guidelines, if needed.

### **3.7.4 Performance Engineering (Production Delivery Level)**

The objective of Performance Engineering is to measure each maintenance (PAM) drop to determine that it meets ACE Performance Requirements.

- a) Review ACE system and engineering designs (including COTS products used within the application), software design, and a selected subset of developed source code and COTS products considered high risk for performance issues, to:
  - Identify performance problems/risks in critical subsystems.
  - Make recommendations for changes that will optimize the software to meet ACE performance requirements.
  - Make recommendations as to how to improve infrastructure performance to meet ACE response time requirements.
  - Verify that the proposed design will meet ACE performance requirements.

- b) Provide services to enhance the existing Performance Benchmark Test. This is limited to augmenting existing test scripts or developing new scripts as needed.
- c) Run the Performance Benchmark Test on every invasive drop, and other PAM drops considered high risk for performance issues, on a test platform commensurate with the performance of the Production system. This will enable the Performance Engineering team to identify problems and work with SW Development to fix problems prior to deployment.
- d) During the Performance Benchmark Test, measure and monitor key application response times and provide recommendations to reduce latency and response time delays.
- e) Provide ACE Production application expertise to EDME for performance analysis of issues identified via EDME's daily performance monitoring of the ACE production application.

#### **Outputs in Addition to Required SLC/SELC Outputs**

- Update the Capacity Planning Modeling Report as needed.
- Document Performance Benchmark Test Results.
- Document Performance Optimization and Design Recommendations.

### **3.7.5 Security Services (Program Level and Production Delivery Level by Subsection)**

The objective of Security Services is to ensure the continued integrity, availability, and confidentiality of the ACE system, as mandated through CBP, DHS, National Institute of Standards and Technology (NIST), and Federal Information Security Management Act (FISMA) requirements.

The Contractor shall follow best practices to achieve this objective, including performing the following activities:

#### **3.7.5.1 Security Activities (Program Level)**

- a) The Contractor shall chair a Security Integrated Product Team (IPT) to discuss, resolve, and coordinate security activities relevant to ACE, so that CBP security service providers are fully in sync on all security issues related to ACE Production and ACE development projects. This will include:
  - Reviewing release designs and PAM change request
  - Validating that security processes exist and are appropriately updated based upon changes being made by the ACE release projects.
  - Identifying the need for security process changes or additions based upon changes made by PAM or by CBP, DHS, NIST, FISMA or other federal mandates
  - Reviewing and confirming that security activities are coordinated among EDME, ENTS, and CSPO, and confirming that such activities are included in the ACE IMS.

- b) The Contractor shall perform Information System Security Officer (ISSO) activities for ACE Development and Test environments. ACE Development and Test environments will not be certified and/or accredited. This will include:
- Validating that processes that monitor user creation, modification, removals, and suspensions on the Development and Test environments are being followed.
  - Reviewing new and updated CBP, DHS, NIST, and FISMA changes to incorporate into all relevant ACE Certification and Accreditation (C&A) documents.
- c) The Contractor shall report any security incident to the CBP Computer Security Incident Response Center (CSIRC) and help with the investigation.
- d) The Contractor shall provide Transport Layer Security (TLS) and Secure Sockets Layer (SSL) certificate documentation for ACE environment use and resolve code signing and DHS server digital certificate issues.

### **3.7.5.2 Security Support Activities (Production Delivery Level)**

- a) The Contractor shall perform ISSO activities for all Certified and Accredited ACE environments (PROD, Disaster Recover (DR), Certification, Training, and the secure enclave). This will include:
- Reviewing new and updated CBP, DHS, NIST, and FISMA changes to incorporate into all relevant ACE C&A documents.
  - Opening risks, as needed, in the DHS-mandated data repository (Trusted Agent FISMA (TAF)) and create Plan of Action and Milestones (POA&Ms) to track their resolution and request DHS waiver/exception for POA&Ms that cannot be resolved within six months. All POA&Ms must be approved by CSPO and reported in the ACE IMS.
  - Validating processes to monitor user creation, modification, removals and suspensions on the ACE production environments exist and are followed.
  - Validating that all processes and procedures that protect the ACE security posture are being followed. Examples include monitoring audit logs on a timely basis.
- b) The Contractor shall perform all necessary activities to support re-certification and accreditation of ACE every three years or when accumulated changes are significant enough to necessitate a re-certification and accreditation, to include but not be limited to updating and delivering prior C&A documents and uploading updated versions into the DHS RMS and TAF.
- c) The Contractor shall review new Production CRs and PTRs that are relevant to security and keep track of such CRs/PTRs for consideration when updating ACE C&A documents. The Contractor shall also provide security requirement updates, security design, and security testing services to implement Production CRs and PTRs.
- d) The Contractor shall conduct an annual security self-assessment audit and request and coordinate with Security Operations Center the Semi-Annual Security Vulnerability

Scans for ACE Production Environments. Conduct analysis of security scan results and create/follow-up on associated POA&Ms, CR, and PTRs.

- e) The Contractor shall support ACE-related security audits and provide the auditors with relevant answers and artifacts in a timely manner.
- f) The Contractor shall provide security oversight for implementing new roles in ACE. Validate that any new or updated roles have only the level of access needed to satisfy the requirement per the latest version of the ACE Security Design document.
- g) The Contractor shall manage and maintain DHS and commercial signed digital certificates used in ACE production systems for secure communications and code signing.
- h) When required the Contractor shall create and coordinate Interconnection Security Agreements (ISAs) and support CBP's development of Memoranda of Understanding (MOUs). The Contractor shall also comply with connections requirements between CBP systems and with other DHS components, as described in CBP and DHS policy directives.

#### **Outputs in Addition to Required SLC/SELC Outputs**

- ACE Annual Security Self Assessment
- Security IPT Minutes and Action Items
- POA&M-related artifacts
- Responses to Audit requests
- Security Design document
- Procedure and Checklist to provide evidence of changes to C&A documents (quarterly)
- Process audit reports for Security Operations Account Management
- Quarterly Report (from Dimensions) of PROD CRs and PTRs showing security impacts, with a notation that the appropriate security documents have been updated

### **3.7.6 Configuration Management (Program Level and Production Delivery Level by Subsection)**

CM uses configuration identification, configuration control, configuration status accounting, and configuration auditing to maintain the integrity of software and physical infrastructure configuration items (CIs).

#### **3.7.6.1 CM Support (Program Level)**

- a) Verify that the following CM activities are performed:

- Version control software (custom-developed and COTS products embedded in the application) configuration Items (CIs), for all ACE environments.
  - Receiving environment CI information from EDME to version control in the ACE CM repository.
  - Obtain appropriate authorization before changed configuration items are entered into the CM system.
- b) Stage ACE-developed applications for the ACE Production environment. Stage all COTS software for all environments.
- Oversee the Contractor’s execution of, adherence to, and compliance with the OIT/CSPO/AST CM policy, plan, processes, and procedures. Participate with the Contractor program and task order leadership to review assessment results and resolve issues regarding CM activities, status, and results.
  - Support reviews to ensure that changes have not caused unintended effects on the baselines (e.g., validate that the changes have not compromised the safety and/or security of the system).

### **3.7.6.2 CM Support (Production Delivery Level)**

The Contractor shall:

- a) Verify change records are in the appropriate state before moving to the production staging area.
- b) Verify that no developed application CI is added, modified, replaced, or removed without an approved request.
- c) Conduct scheduled and emergency builds for developed applications.
- d) Create or release baselines only from configuration items in the CM system and after obtaining authorization from the appropriate change control authority.

#### **Outputs in Addition to Required SLC/SELC Outputs**

- CR and PTR Aging Reports
- Customized Reports per Government request

### **3.7.7 Engineering and Development Tools Administration (Program Level)**

This service provides for the on-going administration and maintenance of the engineering and software development tool set used to design and construct the ACE deliveries. The tools supported by this task include, but are not limited to, the following as well as any underlying prerequisite components (e.g. relational database):

- IBM Rational Build Forge
- IBM Rational Software Analyzer
- Serena Dimensions CM
- Serena Dimensions RM
- Hewlett Packard Quality Center

### **3.7.7.1 Engineering and Development Tools Administration Support Activities (Program Level)**

The Contractor shall perform the following activities in support of the engineering and development tool set for all ACE development projects and the Production Delivery activities.

- a) Perform user provisioning and assignment of authorizations to facilitate the required user access, including Government access as appropriate.
- b) Perform routine product maintenance, to include:
  - Testing and installation of product patches and upgrades, including management of network-based licensing for appropriate products;
  - Support EDME Routine backups and recovery as required; and
  - Periodic cleanup of temporary and log files as required.
- c) Provide services to resolve user issues and problems.
- d) Interface with Commercial off the Shelf (COTS) product vendors to identify and resolve product issues.
- e) Provide services to configure and customize the tools to meet the needs of the ACE development projects, including data and metadata schema configuration.
- f) Maintain awareness of product vendor road maps to identify candidate technology insertion and refresh opportunities and provide these as input to the Architecture and Integration services task for use in COTS life cycle planning.
- g) Perform as the String Owner for the Engineering Support Component (ESC) string which is the string used to host the engineering and development tools.
- h) Provide baseline source code on compact disc (CD) following each [monthly] drop to production. CD must be properly numbered and have the proper affixed label that adheres to security labeling requirements. The CD contents must be encrypted. CDs produced must be inventoried and include the name of the Government representative that received the CD.

## **3.8 ACE Operations & Maintenance (O&M) (Program Level and Production Delivery Level by Subsection)**

### **3.8.1 ACE Level 2 Application Support (ACE Application Analysis and Support) (Production Delivery Level)**

The ACE Application Analysis and Support (Level 2) is the front-line of skilled resources that investigate and respond to reported technical issues with the application. The Level 2 team shall analyze user-related issues, behavioral trends, and the impact of system-related issues within the production environment to support a continuous process improvement model, provide a positive

end-user experience with ACE, and support the maintenance of an optimal level of system availability.

Level 2 is strategically positioned between the Technology Support Desk (TSD or Level 1) and ACE application development teams (PAM Level 3 SMEs/specialists). Level 2 is comprised of resources who perform the initial technical investigation/analysis into incidents to determine the impact on the application, production environment, and user. The team works with other teams as appropriate during the course of incident investigations.

### **3.8.1.1 Level 2 Application Support Activities (Production Delivery Level)**

Level 2 shall perform technical investigation to diagnose user problems and attempt to resolve the problem. If the problem is determined to be the result of developed application code that requires a modification to the baseline in the form of a code change, the problem shall be escalated to Level 3 PAM team for further investigation and resolution. If the problem is determined to be a result of an infrastructure issue, the problem shall be escalated to the Level 3 environments team (EDME) for further investigation and resolution.

Production delivery activities include:

- a) Respond to Sev 1 and Sev 2 trouble tickets. Participate in Root Cause Analysis (RCA) activity for all Sev 1 and Sev 2 incidents.
- b) Provide 24 hours per day, 7 days per week standby/on-call support for Sev 1 and Sev 2 incidents.
- c) Support PAM activities related to maintaining stability to the production environment. While corrective PTRs/CRs are pending approval and implementation, Level 2 shall conduct manual, corrective daily operations in the application (e.g., restart Business Reference Data (BRD) workflows, activate importers on a daily basis, re-push driver or conveyance data, resend Period Monthly Statements (PMS), troubleshoot middleware queues, assist Security Operations with system log research for suspected security violation incidents on an as needed basis and post Portal News items).
- d) Support complementary organizations (e.g., CTOD, Account Services Desk, and TSD) in order to improve standardized, repeatable processes, and provide consistent communications related to application usability. Work closely with other organizations such as Security Operations in troubleshooting account or user ID issues. Level 2 shall investigate problems with the user's Security Data Filter (SDF) roles and privileges. Additionally, Level 2 shall work closely with Port Field Technology Officers (FTOs), Network resources to troubleshoot reported failures in officer safety functions. Level 2 shall investigate the ACE application's role in reported failed alarming incidents.
- e) Participate in end user support conference calls (e.g., the Northern and Southern border conference calls).
- f) Perform daily trend analysis via knowledge gained from end user support conference calls, the field and trade reported trouble tickets, and other user reports to identify potential user/business and technical issues. Provide analysis assessment on a weekly basis.
- g) Support new development efforts by providing subject matter expertise. Assess proposed changes to the production environment for optimal usability and compatibility, and fit with the operational needs of end users.
- h) The team shall collect, analyze, report, and distribute ACE application operational data and reports internally to CSPO Government stakeholders. The team shall capture, analyze and produce the following reports on Level 2 problem resolution activities:

- Incoming ticket rate
  - Ticket closure rate
  - Level 3 ticket escalation rate
- i) The Contractor shall support all performance level objectives defined in Table 3-1 in this SOW.

**Outputs in Addition to Required SLC/SELC Outputs**

- Problem Ticket Metrics and Trend Analysis Assessment (weekly)
- Detailed analysis reports on specific issues (on an as needed basis / upon CBP request)
- Number of trouble tickets in CERT (weekly)

**3.8.2 Electronic Data Interchange (EDI) Support (Program Level and Production Delivery Level by Subsection)**

The ACE EDI team supports the Client Rep branch to support the certification of trade members in using the EDI system to submit electronic manifests and other messages in the ACE Certification environment.

**3.8.2.1 EDI Support (Program Level)**

The Contractor shall:

- a) For ACE ABI CATAIR, review and revise chapters for PSC; make revisions to existing chapters and reference material; respond to Q & A from the trade, CBP client reps and other CBP staff; create new reference material.
- b) For ACE ABI CATAIR Trade Testing Package, create new test scenarios for new ABI transactions; make revisions and updates to the test scenarios, procedures, and 10-90 record comparisons as needed.
- c) For ACE ABI CATAIR, review and revise chapters and reference material: respond to Q&A from the trade, CBP client reps and other CBP staff.
- d) For M1.1 Trade Testing Package, create new test scenarios for new ABI transactions; make revisions and updates to the test scenarios and procedures: assist with issue identification and resolution.

**3.8.2.2 EDI Support (Production Delivery Level)**

The Contractor shall:

- a) Provide production system support, to include monitoring EDI processing, trade participation, system interconnectivity (ACS and ATS on a daily basis:
  - Trade to report problems to the TSD or to Client Reps. Client reps will send email to TSD, copying EDI support and PAM OIT Government leads.
  - Further research into production issues will be via Remedy ticket resolution.
- b) Identify, research, document, create trouble tickets, and create PTRs as needed for EDI processing and portal issues.
- c) Monitor, track, and verify (through testing and research) fixes to issues (internal and external)

- d) Provide Trade Support, to include test and production transaction research, Q & A, and participation in a weekly conference call:
  - Weekly conference call will be conducted by a PAM OIT Government lead. EDI support to be provided as needed (requested by PAM OIT Government lead).
- e) Provide Client Rep Support, to include filer and transaction research, system familiarization, and supporting a weekly conference call (conducted by a PAM Government lead).
- f) Provide CERT system support, to include monitoring and EDI processing verification, EDI filer profiles and accounts, master data maintenance.
- g) Provide support for Census Issues, to include verifying extracts, Q & A, and monitoring issues.
  - Provide support for ACE ABI CATAIR, including revisions to chapters and reference material
- h) Provide support for the Trade Testing Package, including revisions/updates to the test scenarios, procedures, and 10-90 record comparisons as needed.

#### **Outputs in Addition to Required SLC/SELC Outputs**

- EDI sample test data for SWIT (as needed)
- EDI user guide updates (as needed)
- Number of accounts and profiles in CERT (monthly)

### **3.9 ACE Production Application Maintenance (PAM) Services (Program Level and Production Delivery Level by Subsection)**

The PAM team is responsible for maintaining the ACE production application at established performance objectives. The activities included are immediate response, Level 3 (L3) application support, defect correction, application enhancements, and COTS integration.

The Contractor will perform two standard services to support the ACE production application:

- a) **Corrective Maintenance:** There are two forms of corrective maintenance work, both requiring Government authorization via the CSPO Change Control Board: One form is reactive in nature, requiring immediate or near-term action to eliminate existing and known application design, logical and coding errors. The objective of this type of maintenance is to correct problems identified via trouble tickets and PTRs. The second form focuses on activities designed to prevent possible problems from occurring by foreseeing and eliminating application limitations that could pose problems in the future. Examples include eliminating performance bottlenecks not impacting business operations, but are forecasted to become worse over time. Effort expended on this form of corrective maintenance will be determined via Government authorization and is driven by cost, schedule, and risk tolerance.
- b) **Enhancement Maintenance:** Implemented via Government-authorized CRs, the objective of this type of maintenance is to respond to application changes required to either adapt to system environment changes (ex. Upgrades to OS, platform, etc) or to meet the changing needs of users (ex. Business rule changes, changes to legislative ruling, etc.).

Effort expended on enhancement maintenance is driven by cost, schedule, and risk tolerance. Enhancement maintenance recommendations must be approved via the CSPO Review Board.

### **3.9.1 PAM Activities (Program Level)**

#### **3.9.1.1 Delivery Integration (Program Level)**

The Contractor shall:

- a) Escalate PTRs needed by Future Deliveries for development or to successfully execute testing.
- b) Monitor O&M Test String during Delivery Cut Over exercises.
- c) Assist release development teams to understand the changes made to their version of the base line code when merges occur.

#### **3.9.1.2 Support working groups and IPT (Program Level)**

The Contractor shall:

- a) Provide technical support to the Security IPT as requested.
- b) Provide technical support to the Report IPT as requested.
- c) Participate in system resiliency testing.
  - Prepare CRs and PTRs as needed.

#### **3.9.1.3 Problem investigation (Program Level)**

The Contractor shall:

- a) Support performance testing activities.
- b) Support other systems in testing in the development environments as requested by the Government

### **3.9.2 PAM Activities (Production Delivery Level)**

#### **3.9.2.1 Problem investigation (Production Delivery Level)**

- a) The Contractor shall participate in the Root Cause Analysis (RCA) Process and provide the following services:
  - Perform analysis and report to RCA.
  - Work actions items as requested.

- Prepare CRs and PTRs as needed.
- Open and track PMRs with COTS vendors.
- Provide data to vendors upon request.
- Support of DR system via Problem Investigation on the rare occasion an issue falls outside of the DR exercise

### **3.9.2.2 Immediate Response (Production Delivery Level)**

- a) Provide 24x7 on-call response to Production availability incidents.
  - Take Corrective Action to restore service:
    - 1) Implement Government-approved Emergency PTRs to Correct Sev 1 condition.
    - 2) Implement Government-approved Emergency PTRs to correct Sev 2 condition.
    - 3) Perform necessary cleanup activities from Sev 1 and Sev 2 incidents.
    - 4) Provide implementation plan to Configuration Management team.
    - 5) Communicate plan to Government.

### **3.9.2.3 Level 3 (L3) Application Support (Production Delivery Level)**

The Contractor shall:

- a) Process Trouble Tickets that have been escalated from the L2 Application Support Team.
- b) Create Emergency PTRs to resolve Severity 1 issues or at the direction of the Government.
- c) Create PTRs as needed to resolve trouble tickets.
- d) Identify and document in the trouble ticket a suitable workaround to production issues identified in trouble tickets as requested by L2 team.
- e) Provide technical support for L2 technical investigation.
- f) Provide training to the L2 Application Team to implement workarounds for trouble tickets.

### **3.9.2.4 PTR Support (Production Delivery Level)**

#### **3.9.2.4.1 PTR Administration (Production Delivery Level)**

The Contractor shall:

- a) Action production application PTRs (created through trouble tickets) through the full life cycle.
- b) Provide actual effort to resolve each PTR implemented prior to deployment to production.
- c) Provide the Government with the list of open production application PTRs on a monthly basis.
- d) Support the Government to prepare and present PTRs for approval at CSPO Configuration Control Board (CCB).
- e) Prepare clearly written PTRs that explain the impact to the user community, impact to the business process, and frequency of occurrence.

#### **3.9.2.4.2 PTR Implementation (Production Delivery Level)**

The Contractor shall:

- a) Document the design of each PTR prior to implementation.
- b) Develop code and configure COTS products to implement PTRs.
- c) Perform code inspection for every PTR implemented prior to SWIT.
- d) Perform static code analysis of all source code as a standard software development/maintenance activity.

#### **3.9.2.4.3 Unit PTR Testing (Production Delivery Level)**

The Contractor shall:

- a) Prior to SWIT testing, develop and execute unit test cases for each application PTR implemented on the work plan.
- b) Pass inspection of unit test cases prior to execution.
- c) Create data as needed for unit testing.
- d) Document unit test results.
- e) Store and maintain unit test cases and associated unit test results together in the appropriate tool defined by the Government.
- f) Perform peer reviews and inspections on unit test cases and results prior to the start of SWIT.

#### **3.9.2.4.4 SWIT PTR Testing (Production Delivery Level)**

The Contractor shall:

- a) Develop and execute SWIT test cases for each application PTR implemented on the work plan.
- b) Pass peer review and inspection of SWIT test cases prior to execution.
- c) Create data as needed for SWIT testing.
- d) Document SWIT test results.
- e) Store and maintain SWIT test cases and associated SWIT test results together in the appropriate tool defined by the Government.

#### **3.9.2.4.5 Application PTR Builds (Production Delivery Level)**

The Contractor shall:

- a) Provide a list of all PTRs included in a build.
- b) Action PTRs in CM tool to the appropriate state prior to hand off to the build team.
- c) Complete SWIT testing prior to including application modifications in a CM build.
- d) Provide release notes to the CM build team.
- e) Provide and maintain build scripts.

#### **3.9.2.4.6 Application PTR Deployment (Production Delivery Level)**

The Contractor shall:

- a) Coordinate deployment activities with all OIT program office as appropriate.
- b) Provide technical support during application deployments upon request by the Government.

### **3.9.2.5 CR Support (Production Delivery Level)**

#### **3.9.2.5.1 CR Administration (Production Delivery Level)**

The Contractor shall:

- a) Create CRs from approved GIFs, as directed by the CSPO CCB.
- b) Follow the Change Management process.

- c) Provide actual effort to resolve each CR implemented prior to deployment to production.
- d) Provide a project plan for each CR though SWIT completion.

#### **3.9.2.5.2 CR Implementation (Production Delivery Level)**

The Contractor shall:

- a) Follow the standard change control process for all application enhancements.
- b) Develop technical requirements and use cases for CR as needed.
- c) Work with Government SME to develop or modify requirements.
- d) Develop code and configure COTS products to implement CRs.
- e) Document the design of each CR prior to implementation.
- f) Store technical requirements in the tool specified by the Government.
- g) Perform code inspection for every CR implemented prior to SWIT testing.
- h) Perform static code analysis of all source code as a standard software development/maintenance activity.

#### **3.9.2.5.3 Unit CR Testing (Production Delivery Level)**

The Contractor shall:

- a) Prior to SWIT testing, develop and execute unit test cases for each application CR implemented on the work plan.
- b) Pass inspection of unit test cases prior to execution.
- c) Create data as needed for unit testing.
- d) Document unit test results.
- e) Store and maintain unit test cases and associated unit test results together in the appropriate tool defined by the Government.
- f) Perform peer reviews and inspections on unit test cases and results prior to the start of SWIT.

#### **3.9.2.5.4 SWIT CR Testing (Production Delivery Level)**

The Contractor shall:

- a) Develop and execute SWIT test cases for each application CR implemented on the work plan.
- b) Pass peer review and inspection of SWIT test cases prior to execution.
- c) Create data as needed for SWIT testing.
- d) Document SWIT test results.
- e) Store and maintain SWIT test cases and associated SWIT test results together in the appropriate tool defined by the Government.

#### **3.9.2.5.5 Application CR Builds (Production Delivery Level)**

The Contractor shall:

- a) Provide a list of all CRs included in a build.
- b) Complete SWIT testing prior to including application modifications in a CM build.
- c) Provide release notes to the CM build team.
- d) Provide and maintain build scripts.

#### **3.9.2.5.6 Application Deployment (Production Delivery Level)**

The Contractor shall:

- a) Coordinate deployment activities with all OIT program office as appropriate.
- b) Provide technical support during application deployments upon request by the Government.

#### **3.9.2.6 COTS Upgrades (Production Delivery Level)**

The Contractor shall:

- a) Perform Discovery for Upgrades that require application changes.
- b) Implement COTS upgrades following the standard change control process.
- c) Coordinate with EDME for implementation approach verification, and production implementation.
- d) Coordinate with EDME for license control.

#### **3.9.2.7 SAT Support (Production Delivery Level)**

The Contractor shall:

- a) Action PTRs to the appropriate state prior to hand off to SAT team.
- b) Verify O&M Test String operational availability following Application Deployment.
- c) Investigate defects identified by SAT team as approved by the Government.
- d) Fix SAT defects as directed by the Government.
- e) Coordinate the application drops on the O&M String to not impact SAT activities in accordance with the ACE IMS.

### **3.9.2.8 Planning and Coordinating (Production Delivery Level)**

The Contractor shall:

- a) Support the Government to schedule work by providing recommendations to increase efficiency by identifying additional PTRs that are related to planned work.
- b) Make recommendations for communicating roll out of new functionality upon request.
- c) Provide technical input to communicating deployment of new functionality to the production system.

### **3.9.2.9 Systems Engineering Support Activities (Production Delivery Level)**

Prepare National Information Exchange Model Information Exchange Package Documentation (NIEM IEPDs) and Interface Control Documents (ICDs).

#### **Outputs in Addition to Required SLC/SELC Outputs**

- ICD
- IEPD

## **3.10 ROM Effort and Analysis**

The Contractor shall analyze requests and estimate effort (i.e. hours and/or funding) to complete the request prior to beginning work, per Government direction.

- a) Provide estimated effort to address each GIF prior to CR creation.
- b) Provide estimated effort to resolve each CR prior to implementation.

Note: A GIF is required prior to CR creation for any system enhancements. The GIF purpose is to quickly and efficiently vet new system requirements prior to investing additional resources in change request activities.

### **3.11 Communications, Training, Outcomes, and Deployment (CTOD) (Program Level)**

General CTOD activities are detailed in Section 2.5 Communications, Training, Outcomes, and Deployment (CTOD) of the ACE DSRD with the following exceptions:

- a) Section 2.5.3 Stakeholder Communications, in the DSRD, is extended to include the following:
  - Identify organizational impacts associated with changes in business processes resulting from the implementation of the ACE drop. Support the Field Readiness Network and activities performed by that network. Support the ACE project team to help the Field Readiness Network understand the organizational changes associated with the drop.
  - Provide support for the National Port Leadership Information Briefing (PLIB) for each ACE drop.
  - Manage the CBP Role-to-Position mapping process (i.e., mapping and validating system roles to end users).
  - Manage and coordinate the CBP network of ACE Ambassadors to assist with communications to CBP employees, the Trade Community, and other stakeholders as needed.
- b) Section 2.5.5 Field Readiness & Deployment Management, in the DSRD, is eliminated from scope for this SOW.
- c) Legal and Policy references in the following sections of the DSRD are eliminated from scope for this SOW:
  - The reference to Legal and Policy in Section 2.5 Communications, Training, Outcomes and Deployment in the DSRD
  - The reference to Legal and Policy in Section 2.5.1 CTOD Management Leadership in the DSRD
  - Section 2.5.7 Legal and Policy in its entirety in the DSRD is eliminated from scope for this SOW.

## **4. Project Staffing**

The Government prefers to use a teaming delivery model with CBP and ACE Support Team collaborating throughout the project. This teaming model facilitates quality outcomes, reduces the dependency upon inspections, and facilitates knowledge transfer. This may be accomplished through the use of IPTs.

### **4.1 ACE Support Team Resources**

The Contractor shall provide a project team with the appropriate process, technology, and organizational change skills necessary to support this business transformation project. The Contractor shall not hire or utilize new / additional project team members who are not local to

the Washington, DC metropolitan area or who would require out-of-town/state travel without Government approval.

## 4.2 Key Personnel

- (a) The key personnel specified in paragraph (e) below are important to the work being performed hereunder.
- (b) Prior to diverting any of key personnel to other than TO PROD tasks estimated to take 8 hours or longer or cumulatively exceed 8 hours in any calendar month, the Contractor shall notify the Contracting Officer reasonably in advance and shall submit justification (including proposed substitutions, if relevant and necessary as determined by the parties' respective task directors) in sufficient detail to permit evaluation of the impact to this task order. The Contractor may divert such staff upon receipt of the written consent of the Contracting Officer; provided however, that the Contracting Officer may verbally provide such authorization and subsequently confirm it in writing.
- (c) For tasks estimated to take less than 8 hours and cumulatively do not exceed 8 hours in any calendar month, the Contractor is required only to provide advance written notification to the CBP COTR and may proceed without any written form of authorization.
- (d) As appropriate, the list of key personnel may be modified during the term of the task order to either add or delete personnel. All Contractor requests for proposed substitutions must be submitted, in writing, to the Contracting Officer at least fifteen (15) days, [thirty (30) days if security clearances are to be obtained] in advance of the proposed substitutions. All Contractor requests for substitutions must provide a detailed explanation of the circumstances necessitating the proposed substitutions, a complete resume for each proposed substitute, and any other information requested by the Contracting Officer. All Contractor proposed substitutes must have qualifications that are equal to or better than the qualifications of the person being replaced as related to the contract work. The Contracting Officer shall evaluate such requests and promptly notify the Contractor whether the proposed substitution has been approved or disapproved.
- (e) The Contractor shall assign to this Task Order the following key personnel:

- PERSONNEL**
- 1. (b) (4); (b) (6)
  - 2.
  - 3.
  - 4.
  - 5.
  - 6.
  - 7.
  - 8.
  - 9.
  - 10.
  - 11.
  - 12.
  - 13.
  - 14.

15. (b) (4); (b) (6)
16. [REDACTED]

The provisions of this section are unique to this Task Order and supersede, for purposes of this Task Order only, those of section H.2 Key Personnel of the Prime Contract.

### **4.3 Transition Support**

No later than six weeks prior to the expiration date of this task order and upon request by the Government, The Contractor shall participate in and support transition activities to a receiving party, whether a new vendor or a Government team., at the termination of the contract and as required by the Government. This effort will be considered for earned value purposes to be non-measurable effort.

## **5. Acceptance Criteria**

CBP will measure against acceptance criteria to assess the degree to which the Contractor meets desired outcomes and observable objectives. CBP will work with the Contractor to establish specific acceptance criteria to be used for evaluation of the Contractor's performance.

## **6. Accessibility Requirements (Section 508 Compliance)**

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then “1194.21 Software” standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 – 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 1194.25 – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.

36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 – Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional Performance Criteria”, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that 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 approval from the

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

36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

36 CFR 1194.3(f) – Back Office, applies to any EIT item that will be located in spaces frequented only by service personnel for maintenance, repair, or occasional monitoring of equipment. This exception does not include remote user interfaces that are accessible outside the enclosed “space”.

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).

## **7. Deliverables and Delivery Schedule**

Appendix A summarizes the minimum set of deliverables required under this SOW including the due date. The Contractor shall deliver documents in accordance with the terms of the prime contract as well as any additional instructions in the task order. The Contractor’s deliverables shall be under configuration management and stored and maintained in Dimensions. The Contractor shall provide access to a subset of this repository via ModNet to include but not be limited to statements of work, gate review briefings, and plans. These links will be updated promptly and dynamically to reflect the latest document version.

Document delivery within the context of this SOW means that the documents described herein will have been peer-reviewed and approved prior to submission.

## **8. Contractor-Furnished Materials & Other Direct Costs**

### **8.1 Escrow**

The Contractor shall comply with the escrow requirements in Section H.21 of the Contract— Documentation, Escrow, and Code Deliverables.

### **8.2 Tools**

The Contractor shall not use proprietary tools and applications without prior CBP approval. If any proprietary tools are used, the Contractor shall furnish sufficient copies of the tools, the

corresponding documentation, and a license for unlimited right to use by CBP and its duly appointed agents.

## **9. Travel**

The Contractor shall identify the estimated level of travel needed to perform this Task Statement.

## **10. Period of Performance**

Subject to the availability of funding, the period of performance for the activities described in this task statement shall be May 7, 2011 through April 29, 2012

## **11. Place of Performance**

The majority of the work will be performed at various locations in the Washington, DC metropolitan area.

## **12. Security**

Security Section is included in IBM's base contract Tc-2001-025 under Section H.14. No Government data will be processed by non-cleared Contractor personnel on Contractor equipment (Desktop, etc.) or at the Contractor's facility.

### **12.1 Security Review and Reporting**

- (a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.
- (b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the Office of Inspector General, CBP Information Systems Security Manager (ISSM), and other Government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

## 12.2 Interconnection Security Agreements

Interconnections between DHS and non-DHS IT systems shall be established through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both Designated Approval Authorities (DAAs) or by the official designated by the DAA to have signatory authority.

## 12.3 Security Requirements for Unclassified Information Technology Resources

- (a) The Contractor shall be responsible for 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.
  - Within 90 days after the POP start date, 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.
  - 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; 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.
  - 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:
  - Acquisition, transmission, or analysis of data owned by DHS with significant replacement cost should the Contractor's copy be corrupted.

- Access to DHS networks or computers at a level beyond that granted the general public (e.g., 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 six months after POP start date, 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.

## **12.4 Contractor Employee Access**

- (a) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the COTR will arrange and complete any nondisclosure agreement furnished by DHS.
- (b) The Contractor shall have access only to those areas of DHS IT 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.
- (c) 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).
- (d) 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.
- (e) 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:

- The individual must be a legal permanent resident of the United States 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.
  - There must be a compelling reason for using this individual as opposed to a U. S. citizen.
  - The waiver must be in the best interest of the Government.
- (f) 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.

## **12.5 Information Security (ISO) Compliance**

All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD 4300.1, *Information Technology Systems Security Program and 4300A Sensitive Systems Handbook*.

## **12.6 Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information**

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

## **13. Engineering Platforms**

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

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

## **14. Enterprise Architecture Compliance**

The Offeror shall ensure that the design conforms to the DHS and CBP enterprise architecture (EA), the DHS and CBP technical reference models (TRM), and all DHS and CBP policies and guidelines as promulgated by the DHS and CBP CIOs, Chief Technology Officers (CTO) and Chief Architects (CA) such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture Technical Framework.

The Offeror shall conform to the federal enterprise architecture (FEA) model and the DHS and CBP versions of the FEA model as described in their respective EAs. Models will be submitted using Business Process Modeling Notation (BPMN 1.1, BPMN 2.0 when available) and the CBP Architectural Modeling Standards for all models. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles as reflected by the hardware software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software and infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal technology insertion process which includes a trade study with no less than four alternatives, one of which shall reflect the status quo and one shall reflect multi-agency collaboration. The DHS/CBP TRM/standards profile will be updated as technology insertions are accomplished.

All developed solutions shall be compliant with the HLS (Homeland Security) EA.

All IT hardware or software shall comply with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model. Submittal shall be through the CBP Data Engineering Branch and 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 TOs shall be IPv6 compatible without modification, upgrade, or replacement.

#### Dependencies:

1. All DHS and CBP policies and guidelines promulgated by the DHS and CBP CIOs, CTOs, and Chief Architects that are applicable to this task are specifically identified and will be made available electronically within five days of POP start date. Subsequent updates or newly drafted items will be made available electronically within 10 days of publication or applicability, whichever is earlier.
2. The Contractor is only responsible for preparing materials to be submitted to the Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model. Submission to EDMO will be performed by CSPO Government representatives.
3. CBP Modeling Standards applicable to ACE will be specifically identified and will be made available electronically within five days of POP start date. Subsequent updates or newly drafted items will be made available electronically within ten days of publication or applicability, whichever is earlier.

#### Assumptions:

1. Migration to the Common Enterprise Services (CES) Single Sign-on Portal is assumed to be a strategic activity contracted outside the scope of this task order. No effort is included in this task to support this migration. This task will conform to the ACE architecture and relevant integration with the Single Sign-on Portal in place in ACE production at the time of contract award.
2. Integration with the CES CBP Enterprise Service Bus (ESB) will only be performed for service interfaces that have been mutually agreed upon by CBP and the Contractor. Existing interfaces will not be rebuilt nor modified to integrate with the ESB.
3. Conformance to the HLS EA is assumed when a release is found to be compliant with the CBP EA by the CBP AAA review at a specific SELC gate. No effort will be expended in directly addressing DHS HLS EA compliance criteria.
4. Conformance to the Federal Enterprise Architecture (FEA) model and DHS and CBP versions of the FEA model is assumed when a release is found to be compliant with the CBP EA by the CBP AAA review at a specific SELC gate. No effort will be expended in directly addressing FEA compliance criteria.
5. Draft and “in-progress” and otherwise unapproved policy, guidelines, and standards are not binding unless specifically identified and made available. The version made available will be assumed to be current until another version is provided. Additions and modifications may require the invocation of the formal change management process to assess the potential impact.

6. Business Process Modeling Notation (BPMN) standards for business process models will be used to the extent they are supported by available, approved modeling tools. Any deviations from or additions to standards will be identified by Contractor.
7. Unified Modeling Language (UML) is assumed to be an acceptable notation for application design models. The limitation of the use of UML 2.0 to only infrastructure is assumed to be applicable only to the development of business process.
8. The specific version of the NIEM standard to be followed is NIEM 2.0.
9. The requirement for the use of NIEM to describe data semantics is applicable only to data interfaces with other systems, and does not apply to the description of persistent data stores within the ACE system or data interchanges between ACE application components.
10. CBP list of currently approved products and standards if required as is access to the list of products and standards currently under consideration. The latter is required to ensure that any potential technology insertions are not duplicative and collaboration among all interested parties is ensured.
11. Support of the Transition Plan for production system migration at a DHS data center is assumed to a strategic activity contracted outside the scope of this task order. No effort is included in this task to support any activities related to this transition plan. This task will conform to the ACE architecture and relevant data center strategy in place for the ACE production at DR systems at the time of contract award.

## **15. Transition Plan**

The DHS CIO has established portfolio targets for the IT infrastructure that include production system consolidation at a DHS data center, and transition to OneNet. The Contractor must be prepared to support CBP Government leads, within the purview of this task order, to provide any required transition planning or program execution, associated with meeting the agreed to transition timeline, as directed by Government personnel. This includes the following types of tasking:

- Coordination with Government representatives.
- Review, evaluation, and transition of current support services.
- Transition of historic data to new Contractor system.
- Government-approved training and certification process.
- Transfer of all necessary business and/or technical documentation.

- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, business processes, equipment, furniture, phone lines, and computer equipment.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance.
- Applicable debriefing and personnel out-processing procedures.

## **16. Program Management Tool for Reporting**

### **Use of CBP's designated program management tool for reporting purposes**

The Contractor shall perform program and project planning and management duties to facilitate the development of the system and operational requirements for the task elements. This will include, but is not limited to, the preparation of plans and schedules based on technical and project data; tracking program funds; scheduling and conducting technical and planning meetings; conducting project reviews; and preparing status reports. This includes entering program related information in CBP's designated Program Management tool.

The CBP designated Program Management tool is required to accomplish the following:

- Manage CBP/CIO resources both effectively and efficiently from an enterprise-wide standpoint.
- Plan the development of new investments and projects in support of agency goals and objectives.
- Ensure that investment and projects are being managed within specified cost, schedule, and performance parameters.
- Foster the development of effective corrective action plans when needed.

Within seven days of receiving the Confidentiality Agreement, the Contractor must have its staff assigned to CBP sign the agreement agreeing to the confidentiality provisions imposed by the Program Management tool licensor.

The Contractor shall be familiar with this tool and enter, update, track, and report associated contract activities, as directed by the Program Office Task Monitors or the COTR, within the CBP designate. If support is required to use the tool, the Contractor will contact the Program Manager Task Monitors or the COTR directly, and will not attempt to seek support from the Program Management tool licensor directly.

## 17. Government Project Leadership Contacts

### Executive Director:

Name: (b) (6)  
Telephone: (b) (6)  
Email: (b) (6)@cbp.dhs.gov

### Task Monitor:

Name: (b) (6)  
Telephone No: (b) (6)  
Email: (b) (6)@dhs.gov

### Task Monitor (Level 2 Application Support):

Name: (b) (6)  
Telephone No: (b) (6)  
Email: (b) (6)dhs.gov

### COTR:

Name: (b) (6)  
Telephone No: (b) (6)  
Email: (b) (6)dhs.gov

### Contracting Officer:

Name: Michael P. Rebain  
Telephone No: (b) (6)  
Email: (b) (6)@dhs.gov

## Appendix A. Required Artifacts Table

Artifacts are required documents defined as outputs in this SOW.

**Table A-1 Required Artifacts**

#	Artifact Title	Delivery Schedule	Area
1.	TO PROD schedule (of all activities) to be incorporated into the IMS	Weekly	Task Order Management (3.3)
2.	Data Updates for input into the Monthly CSPO PMR and CPR	Monthly	Task Order Management (3.3)
3.	Consolidated Team Lead Status Report	Weekly	Task Order Management (3.3)
4.	PAM Performance Measure Results as described in Table 3-1	Refer to Table 3-1	Quality Assurance (3.6)
5.	ACE High-Level Architecture Description and Diagram	As required per development contracts	ACE Architecture and Integration (3.7.1)
6.	ACE Operational Model (Logical)	As required per development contracts	ACE Architecture and Integration (3.7.1)
7.	ACE High-Level Data Model	As required per development contracts	ACE Architecture and Integration (3.7.1)
8.	ACE Data Dictionary	As required per development contracts	ACE Architecture and Integration (3.7.1)
10.	ACE COTS Roadmap (for engineering and software development tools used to design and construct the ACE application)	Quarterly	ACE Architecture and Integration (3.7.1)
12.	Inputs to the EDME COTS Roadmap (as required)	As required per Government request and as required per development contracts	ACE Architecture and Integration (3.7.1)
13.	Technology Insertion Requests (as required)	As required per Government request	ACE Architecture and Integration (3.7.1)
14.	Trade Studies (as required)	As required per Government request	ACE Architecture and Integration (3.7.1)
15.	Prototypes and proof of concepts	As required per Government request	ACE Architecture and Integration (3.7.1)
16.	Briefings and Reports (as required)	As required per Government request	ACE Architecture and Integration (3.7.1)
17.	ACE Database Data Management Plan	As required per development contracts	ACE Architecture and Integration (3.7.1)
18.	Weekly status report to Task Order	Weekly	ACE Architecture and Integration (3.7.1)

#	Artifact Title	Delivery Schedule	Area
	Management		
19.	Business Process Hierarchy updates (at gate reviews)	As required per development contracts	Systems Engineering Leadership and Governance Services (3.7.2)
20.	Government Ad hoc request responses	As required per Government request	Systems Engineering Leadership and Governance Services (3.7.2)
21.	Systems Engineering Practices, Processes, and Procedures synchronized with CBP SELC	As required	Systems Engineering Leadership and Governance Services (3.7.2)
22.	Ad hoc reports per Government request	As required per Government request	Systems Engineering Leadership and Governance Services (3.7.2)
23.	Requirements baselines (at gate reviews)	As required per development contracts	Systems Engineering Leadership and Governance Services (3.7.2)
24.	Interface Control Documents (ICD)	As required per development contracts	ACE Production Application Maintenance (PAM) Services (3.9)
25.	Information Exchange Package Documentation (IEPD)	As required per development contracts	ACE Production Application Maintenance (PAM) Services (3.9)
27.	Software development process defining use and enforcement of static code analysis	As required	Software Engineering Leadership and Governance Services (3.7.3)
28.	Update the Capacity Planning Modeling Report as needed	As required per PAM drops	Performance Engineering (3.7.4)
29.	Document Performance Benchmark Test Results	As required per PAM drops	Performance Engineering (3.7.4)
30.	Document Performance Optimization and Design Recommendations	As required per PAM drops	Performance Engineering (3.7.4)
31.	ACE Annual Security Self Assessment	Annual	Security Services (3.7.5)
32.	Security IPT Minutes and Action Items	Every 2 weeks	Security Services (3.7.5)
33.	POA&M-related artifacts	As required	Security Services (3.7.5)

<b>#</b>	<b>Artifact Title</b>	<b>Delivery Schedule</b>	<b>Area</b>
34.	Responses to Audit requests	As required	Security Services (3.7.5)
35.	Security Design document	As required or in accordance with development schedules in the ACE IMS	Security Services (3.7.5)
36.	Procedure and Checklist to provide evidence of changes to C&A documents (quarterly)	Quarterly	Security Services (3.7.5)
37.	Process audit reports for Security Operations Account Management	Weekly	Security Services (3.7.5)
38.	Quarterly Report (from Dimensions) of Production CRs and PTRs showing security impacts, with a notation that the appropriate security documents have been updated	Quarterly	Security Services (3.7.5)
39.	CR and PTR Aging Reports	Monthly	Configuration Management (3.7.6)
40.	Customized Reports per Government request	As required per Government request	Configuration Management (3.7.6)
41.	Problem Ticket Metrics and Trend Analysis Assessment (weekly)	Weekly	ACE O&M (3.8)
42.	Detailed analysis reports on specific issues (on an as needed basis / upon CBP request)	As required per Government request	ACE O&M (3.8)
43.	EDI sample test data for SWIT (as needed)	As required per Government request	ACE O&M (3.8)
44.	EDI user guide updates (as needed)	As required per Government request	ACE O&M (3.8)
45.	Number of accounts and profiles in CERT (weekly)	Weekly	ACE O&M (3.8)