AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	PAGE OF PAGES 1 | 2

2. AMENDMENT/MODIFICATION NO.	3. EFF. DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
P00013	02/07/2013	0020067114	

6. ISSUED BY CODE 70050800
DHS - Customs & Border Protection
Customs and Border Protection
1300 Pennsylvania Ave, NW
Procurement Directorate - NP 1310
Washington DC 20229

7. ADMINISTERED BY (If other than Item 6) CODE
DHS - Customs & Border Protection
Customs and Border Protection
1300 Pennsylvania Ave, NW
Procurement Directorate - NP 1310
Washington DC 20229

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and Zip Code)
LOCKHEED MARTIN MISSION
700 N FREDERICK AVE
SYSTEMS
GAITHERSBURG MD 20879-3328
CODE 000000000 FACILITY CODE

9A. AMENDMENT OF SOLICITATION NO.
9B. DATED (SEE ITEM 11)
10A. MODIFICATION OF CONTRACT/ORDER NO. / HSBP1009J27216
10B. DATED (SEE ITEM 13) 08/01/2009

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)
SEE ATTACHED DOCUMENT

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

☐ A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

☐ B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (Such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103 (b).

☐ C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

☒ D. OTHER (Specify type of modification and authority)
52.243-3 CHANGES TIME-AND-MATERIALS OR LABOR HOURS

E. IMPORTANT: Contractor ☒ is not ☐ is required to sign this document and return _____ copies to issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to add an additional hours for a Subject Matter Expert/Process Improvement Support III and funding in the amount of $149,482.00 to cover an additional [redacted] hours at a rate of [redacted] from February 2013-May 2013; and [redacted] hours at a rate of [redacted] from June 1, 2013-July 31. 2013.

The task order is hereby modified as follows:

1. Mod P00013 is funded in the amount of $149,482.00.

2. Total task order value is increased FROM: $3,717,664.38 BY: $149,482.00 TO: $3,867,146.38

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
		EARL J. LEWIS III Contracting Officer	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY [redacted]	16C. DATE SIGNED 2/8/13

NSN 7540-01-152-8070
PREVIOUS EDITION UNUSABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA FAR (48 CFR) 53.243

14. DESCRIPTION OF AMENDMENT/MODIFICATION (*Organized by UCF section headings, including solicitation/contract subject matter where feasible.)*

3. Reference: The updated SOW

All other terms and conditions remain unchanged.

ATTACHMENT INFORMATION
FOR
AWARD/ORDER/IA MODIFICATION: HSBP1009J27216P00013

I.1 SCHEDULE OF SUPPLIES/SERVICES

ITEM #	DESCRIPTION	QTY	UNIT	UNIT PRICE	EXT. PRICE
10	ELCM/PAL Support	1.000	AU	(b) (4)	
20	Option 1 - ELCM & PAL Support	1.000	AU		
30	WSPO-Option 2	1.000	AU		
40	PM Education Support-Option 2	1.000	AU		
50	Additional PM Education Support Option 2	1.000	AU		
60	PM Education Support - Modification	1.000	AU		
70	PM Education Support - Modification	1.000	AU		
80	WSPO Support	1.000	AU		
90	PMB PI Support	1.000	AU		
100	PMB PI Support - DHS PM Track	1.000	AU		
110	PMB PI Support - DHS PM Track	1.000	AU		
120	Additional PMB PI Support - DHS PM Track	1.000	AU		
130	WSPO Support	1.000	AU	$149,482.00	$149,482.00

Total Funded Value of Award: **$3,867,146.38**

I.2 ACCOUNTING and APPROPRIATION DATA

ITEM #	ACCOUNTING and APPROPRIATION DATA	AMOUNT
10	6100.2525USCSGLCS0923030000Z00009400HQ01 IR2342525	(b) (4)
20	6100.2525USCSGLCS0923030000Z65Q10400HQ01 IR2342525	
30	6100.2525USCSGLCS0923030000Z65Q09173SB03 IU2012525	
40	6100.2525USCSGLCS0923030000Z65Q11400HQ01 IR2342525	
50	6100.2525USCSGLCS0923030000ZJU211111R0HQ01 IR2342525	
60	6100.2525USCSGLCS0923030000Z00012400HQ0106052401 IR2342525	
70	6100.2525GLCS0923030000ZJU312124R0HQ01 IU2012525	
80	6100.2525USCSGLCS0923030000Z00012173SB0301031600 SB7012525	
90	6100.2525USCSGLCS0923030000Z00012400HQ0106052401 IR2342525	
100	6100.2525GLCS0923030000ZJU312124R0HQ01 IU2012525	
110	6100.2525USCSGLCS0923030000Z00012400HQ0106052401 IR2342525	
120	6100.2525GLCS0923030000ZJU312124R0HQ01 IU2012525	
130	6100.2525USCSGLCS0923030000Z00010173SB031502A600 SB7012525	$149,482.00

I.3 DELIVERY SCHEDULE

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
Customs and Border Protection 1300 Pennsylvania Avenue N W Washington, DC 20229	10	1.000	07/31/2010
Customs and Border Protection 7681 Boston Blvd Springfield, VA 22153	20	1.000	07/31/2011
	30	1.000	07/31/2012
	40	1.000	07/31/2012
	50	1.000	10/01/2011
	60	1.000	07/31/2012
	70	1.000	07/01/2012
	80	1.000	07/31/2013

DELIVER TO:	ITEM #	QTY	DELIVERY DATE
	90	1.000	07/31/2013
	100	1.000	07/31/2013
	110	1.000	08/01/2012
	120	1.000	09/05/2012
	130	1.000	01/03/2013

Systems Engineering Life Cycle & Project Management Maturity, Process Improvement, Enterprise Life Cycle Methodology, and Process Asset Library Support Statement of Work

HSBP 1009J27216
Modification to add hours/funds to Subject Matter Expert/Process Improvement Support (III) Labor Category
Option Period 3 of 4

February 1, 2013

Table of Contents

1.0 Overview 1
2.0 Scope of Work 1
3.0 General Requirements and Background Information 2
4.0 Key Personnel 2
5.0 Labor Category Functions 3
5.1 Staffing History 3
5.2 Activities and Tasks by Position 3
6.0 Deliverables and Delivery Schedule 8
6.1 Acceptance 8
6.2 Table of Deliverables and Work Products 8
6.3 Dependencies 9
6.4 Review 9
6.5 Delivery Methods 9
6.6 Formats 9
6.7 Performance Standards 9
7.0 Government Furnished Equipment and Materials 14
7.1 Government Furnished Equipment 14
7.2 Government Furnished Materials 14
8.0 Contractor Furnished Materials and ODCs 14
9.0 Accessibility Requirements (Section 508 Compliance) 14
9.1 Accessibility Requirements (Section 508) 14
9.2 Section 508 Applicable EIT Accessibility Standards 14
9.3 Section 508 Applicable Exceptions 15
9.4 Section 508 Compliance Requirements 15
10.0 Enterprise Architecture (EA) Compliance 16
11.0 ISO (Information Security) Compliance 17
11.1 General Information Security Clause 17
11.2 Interconnection Security Agreements 17
11.3 3052.204-70 Security Requirements For Unclassified Information And Technology Resources (JUN 2006) 17
11.4 CONTRACTOR EMPLOYEE ACCESS (JUN 2006) 18
11.5 Security Certification/Accreditation 21
11.6 Disaster Recovery Planning & Testing – Hardware 21

11.7 Security Review and Reporting 22

11.8 Access to Unclassified Facilities, Information and Technology Resources, and Sensitive Information 22

11.9 OMB-M-07-18 FDCC 22

11.10 Personal Identification Verification (PIV) Credential Compliance 23

11.11 Encryption Compliance 23

12.0 Contractor Signature Format *24*

13.0 Period of Performance *24*

14.0 Place and Hours of Performance *24*

14.1 CBP Locations 24

14.2 Telecommuting 24

14.3 Work Hours 25

14.4 Overtime 26

14.5 Observance of Legal Holidays and Excused Absence 26

15.0 Travel and Other Direct Costs *26*

16.0 Billing and Invoices *26*

16.1 Invoice Content 26

16.2 Invoicing Submission and Deadlines 27

17.0 Government Contacts *27*

17.1 Executive Lead 27

17.2 Contracting Officer's Representative (COR) 27

17.3 Alternate COR 27

1.0 Overview

U.S. Customs and Border Protection (CBP) is modernizing its business processes, information and technology (IT) systems, and infrastructure to provide functionality needed to support its mission and to build and use the new Office of Information and Technology (OIT), CBP and Department of Homeland Security (DHS) Enterprise Infrastructure. This initiative involves applying the CBP Enterprise Life Cycle Methodology (ELCM), the Process Asset Libraries (PALs), the Online DHS and CBP System Engineering Life Cycle (SELC), and DHS project management discipline to integrate all DHS organizations and multiple projects and activities into a comprehensive and integrated approach to creating and using mature Industry Best Practices.

The purpose of this procurement is to obtain development, training, and process improvement services to operate and maintain the OIT ELCM Tool Suite consisting of the ELCM, the Online DHS SELC, and the CBP PALs.

The Tool Suite provides the mechanisms for managing, updating, and improving the CBP/OIT Process Baseline. Improved practices, workflows, and improvement opportunities shall be developed, and published using the ELCM Tool Suite to address "pain points" and introduce disciplined Industry Best Practices based on government and industry improvement models.

2.0 Scope of Work

The scope of this contract is to provide support for DHS and CBP project and program integration and to perform enhancement, operational and maintenance support of the complex OIT ELCM Tool Suite. The following aspects to the services are required:

- The administration of process and project management implementation
- Development, programming, and enhancement of the ELCM Tool Suite within the enterprise collaboration tool
- Support CBP implementations of the PAL Tool for CBP OIT, Office of Administration (OA) and Office of Technology Innovation and Acquisition (OTIA)
- Support, mentor, and train DHS/CBP PAL/ELCM users as required on ELCM Tool Suite and SELC
- Integrate DHS SELC within CBP
- Provide thought leadership and senior level guidance on IT service management and systems development
- Assist in development of process assets, including establishing program office and branch processes and procedures
- Review program office and branch processes and procedures to verify compliance with DHS, CBP, and OIT standards as well as incorporating best industry practices from other sources
- Assist with tailoring individual project plans, on the Microsoft Project Server, in accordance with the approved Program and Project Tailoring Matrixes
- Review project documentation for compliance with the SELC, as tailored for projects
- Provide expertise in developing and delivering project management and SELC education

3.0 General Requirements and Background Information

The Contractor shall integrate with the OIT and other CBP and DHS activities. Activities include support of process integration and the enterprise vision/goals, process baseline management, mentoring and training, and process integration, and asset development.

This effort shall integrate management of the OIT Process Baseline through the ELCM Tool Suite; enabling ongoing architecture modernization, organizational process improvement activities, and workflows consistent with the Federal Enterprise Architecture (FEA), Integrated Capability Maturity Model (CMMI©), ITIL©, and Project Management Book of Knowledge© (PMBOK) among other guiding models.

The Contractor shall provide mentoring, demonstrations, presentations, and discussions, thought leadership, and assistance on ELCM, process integration, and repository issues, at the request of CBP, DHS, and other customers.

The Contractor shall align the Process Baseline with Chief Information Officer (CIO), Enterprise Architecture Review Board (EARB) and Deputy Directors' Council (DDC) priorities, pain-points, strategies and opportunities. Enhancements shall be focused on supporting OIT Process Integration, SELC Project/Program Support (tailoring, status, link to project artifacts, training), and enhanced process flow display. Other enhancements shall address project views and feedback. Additionally, the Contractor shall be required to:

- Manage and Execute ELCM Tool Suite Changes
- Develop and implement formal ELCM Tool Suite Training
- Update ELCM Computer Based Training (CBT) and Orientation Training
- Perform ELCM Gap Analysis

4.0 Key Personnel

Contractor employees designated as key personnel for this Task Order are listed as follows:

Table 1 – Key Personnel

EAGLE Labor Category	Level	No. of Positions
(b) (4)		

The key personnel specified in Section 4.0 are considered essential to the work being performed under this contract. During the first sixty (60) days of the task order, the Contractor shall not make any key personnel changes unless an individual's sudden illness, death or termination of employment necessitates such substitutions. In case of theses occurrences, the

Contractor shall notify the Contracting Officer and Contracting Officer's Representative (COR) promptly and submit documentation pertaining to the proposed substitution in writing.

Before removing or replacing any of the specified individuals, the Contractor shall notify the COR, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action in order to enable the COR to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel until the COR approves the change.

5.0 Labor Category Functions

5.1 Staffing History

The following table presents changes in staffing hours based on expected budget changes

Table 2 – Staffing Hours

Position	Base Year	Option 1 of 4	Option 2 of 4	Option 3 of 4
[redacted]				

(b) (4)

ELCM/OIT PAL development schedule will be elongated.

5.2 Activities and Tasks by Position

This project has a diverse history. Based on this history, the following sections describe the types of tasks and activities associated with each position.

5.2.1 Information Technology Senior Consultant/Solution Engineering

- Perform ELCM/PAL Solution Engineering to include evaluating complex requirements, performing root cause analysis, and producing recommended system solutions. All solutions recommendations shall be documented appropriately.

- Perform ELCM Tool Suite software configuration and change management, including participation in configuration control boards, processing change requests, and coordinating with technical support organizations.
- Prepare, analyze, and deliver technical requirements and problem reports, including PTR responses and recommended software and hardware specifications
- Integrate and deliver DHS, CBP, and OIT strategic priorities in a Requirements Traceability Matrix
- Prepare and deliver test procedures and test reports for software releases

5.2.2 Information Technology Senior Consultant/SELC Support

- Analyze the current contents of the OIT PAL for gaps and overlaps in the existing Enterprise process assets and practices using CMMI, ITIL, PMBOK, FEA and any other applicable maturity models.
- Integrate Process gap analysis with DHS, CBP CIO, ARB, and DDC priorities, pain points, and strategies.
- Maintain the integrity of the OIT Process Baseline
- Ensure that Enterprise process assets in the OIT PAL are linked to the correct place(s) in the ELCM Tool Suite
- Provide expert consultation services to senior OIT management in identifying key process areas that need to be addressed.
- Mentor key ELCM Tool Suite users.
- Update Agile Overview training based on student feedback, in support of OIT's Enterprise Transition to Agile. Assist the Enterprise in their rollout, and adoption of the Framework.
- Prepare and present four hour Agile Overview Training sessions to CBP.
- Each training session will cover introduction to Agile concepts, lessons learned, and tool usage to assist with Agile transition.

5.2.3 Information Technology Senior Consultant/Project Manager

- Perform all aspects of program and technical planning and resource management
- Liaison between Contractor(s), Contracting Officer (CO), and COR as required
- Identify replacements in the event contractor must be replaced

5.2.4 Information Technology Sr. Consultant/PM Education

- Coordinate with DHS component SMEs to compile material relevant for inclusion into the course materials
  - Researching with the SMEs the appropriate directives and information that needs to be elevated and included into the course materials
  - Subsequent analysis of the courses based upon the research conducted
  - Support the customization of courses to apply the appropriate application of the research and analysis into the supplemental materials from the research of DHS polices, directives, tools and guidance
- Incorporate Lessons Learned
- Monitor DHS ITPM Courses to capture lessons learned
- Incorporate lessons learned into next Track course materials

- Identify for incorporation into the ELCM Tool Suite updates based on customization research, and analysis, and lessons learned.

5.2.5 Information Technology Consultant

- Perform CBP ELCM Tool Suite and CBP PAL total life cycle software and database engineering using the following tools and methods

ColdFusion	Toad™
Java Script	AJAX
HTML	XML
ACC Repair (DHS and Section 508 Compliance)	Dreamweaver™
Oracle	IIS
Microsoft Visio (for documentation and flow diagramming)	CSS
Microsoft Office Suite (Word, Excel, and PowerPoint) (for documentation purposes)	.net
MS SharePoint, including 2010	ASP.NET
SharePoint Designer 2010	C#, Visual Basic
Visual Studio 2010	SQL Server 2008

- Perform CBP ELCM Tool Suite and CBP PALs problem resolution including system troubleshooting
- Perform requirements and software analysis throughout the system life cycle.
- Perform ELCM Tool Suite and CBP PALs total life cycle system integration, system maintenance and sustaining engineering to include development, testing, and production environments.
- Perform system, unit and integration testing
- Analyze and prepare technical requirements including recommended software and hardware specifications.
- Support the ELCM Tool Suite vision and mission
- Support ELCM Tool Suite total life cycle technical planning
- Participate in customer technical interchange meetings.

5.2.6 Subject Matter Expert/Senior Executive Consultant (IV)

CBP's OIT PMB is responsible for: documenting and improving OIT's business processes; increasing collaboration among its program offices; develop and maintain the CBP System SELC, knowledge management system and associated artifacts; provide training for CBP employees; support strategic planning and policy; and instituting best practices to aid OIT in achieving its goals and objectives. To support the function of PMB a senior-level Subject Matter Expert (SME) is required to:

- Look across the board spectrum of the organization, identify connections, and tie those connections together in terms with which PMB will be able to better incorporate process and project management principles into the organization and support the mission of CBP.
- Provide support that will enable PMB to, in a timely manner, meet DHS, CBP and OIT senior management high priority initiatives.

- Evaluate expectations for and capabilities of OIT's services and make recommendations for improvement.
- Providing thought leadership and senior level guidance on IT service management and systems development

Qualifications: The candidate must have:

- A sound understanding of the agency, its components/offices, and initiatives; a plus if direct experience with agency mission/business organizations
- 15+ years of demonstrable knowledge, experience, and leadership in business process improvement and re-engineering, strategic planning and policy, and System Development Life Cycle. Education cannot be used as a substitution for experience.
- Knowledge and experience of federal program and investment initiation, management and compliance with applicable laws and regulations, e.g. Government Performance Results Act of 1993, Information Technology Management Reform Act of 1996, Government Paperwork Elimination Act of 1998, E-Government Act of 2002, Homeland Security Acquisition Management and FAR Part 10 guidance for Market Research Plan, etc...
- Mastery/expertise in business process improvement and re-engineering, enterprise architecture, planning and policy, and DHS SELC.

Key Requirements: The candidate must:

- Be a U.S. Citizen or National
- Have an active CBP Full Background Investigation clearance

5.2.7 Subject Matter Expert /Process Improvement Support (III)

- Assist with tailoring individual project plans, on the Microsoft Project Server, in accordance with the approved Program and Project Tailoring Matrixes
- Establish program office processes and procedures
- Review program office processes and procedures to verify compliance with all applicable standards
- Establish organization processes and procedures
- Review organization processes and procedures to verify compliance with all applicable standards
- Review project documentation for compliance with the SELC, as tailored for the project

5.2.8 Subject Matter Expert/SELC Education

- Refine requirements for a DHS SELC training course
- Prepare DHS SELC training course for inclusion in the DHS Program/Project Management Initiative
- Deliver DHS SELC training course to DHS personnel
- Participate in DHS SELC training course working groups/meetings
- Refine DHS SELC training course based on feedback from working groups, training participants and DHS management

5.2.9 Subject Matter Expert/Outreach and Strategic Planning

- Providing thought leadership and senior level guidance on:
- EDME Service Strategy Development and alignment
- EDME Service Performance analysis and Reporting
- EDME Service Strategy Process Management
- Support OIT Strategy development

5.2.10 Business Process Re-engineering Specialist/Training Coordinator

- Catalog all submissions to the ELCM and OIT PAL under the correct organizations and process domains.
- Maintain integrity of the OIT Process Baseline
- Assist in linking process assets in the OIT PAL to the correct place(s) in the ELCM Tool Suite
- Assist submitters with using the OIT MSWord formats and templates.
- Review all submissions to the ELCM and OIT PAL for adherence to OIT standard formats and templates.
- Provide overall training support to the DHS Information and Technology Project Management Track Education Program.
    - Tracking overall maintenance of the Education Program
    - Provide administrative logistics associated with course delivery
    - Coordinate with students, print shop, training vendors, etc. in preparation for set-up as well as close down of courses
    - Maintain PM Education SharePoint Site specific to record keeping and course updates
    - Perform general administrative activities as required

5.2.11 Subject Matter Expert/Process Improvement Support (II)

- Provide expert consultation services to senior OIT management in identifying key process areas to be addressed
- Create and maintain process flow mapping of how OIT processes are completed from input to output by specific tasks
- Develop process assets including complete description, metrics, and supporting assets
- Analyze and maintain the OIT Process Baseline and DHS/CBP Systems Engineering Life Cycle (SELC) including alternative life cycles, system configuration, system reporting, and recommended process improvement
- Analyze the current contents of the OIT PAL/ELCM for gaps and overlaps in the existing enterprise process assets and practices using CMMI, ITIL, PMBOK, FEA and other applicable maturity models
- Integrate process gap analysis with DHS, CBP CIO, ARB, and DDC priorities, pain points, and strategies
- Mentor key OIT PAL and ELCM Tool Suite users on process improvement, OTI PAL, ELCM, and Systems Engineering Life Cycle (SELC) best practices
- Prepare and present status reports

6.0 Deliverables and Delivery Schedule

6.1 Acceptance

Acceptance of a deliverable or work product occurs when the Executive Lead accepts via written notification sent to the Contractor. Contractor shall then work with the Executive Lead to obtain the appropriate management approvals for deployment to the organization.

6.2 Table of Deliverables and Work Products

A table of deliverables that summarizes the minimum set of deliverables required under this contract is found in Table 3, Deliverables and Work Products. The draft and interim deliverables shall be in the formats recommended by the Contractor and agreed to by CBP. The Contractor may propose other products deemed necessary or appropriate. Documents are to be delivered in accordance with the terms of the Statement of Work as well as any additional instructions specified by the contract.

Table 3 – Deliverables and Work Products

No.	Deliverable	Person Responsible	Description	Due Date
1	SELC Training Materials	Subject Matter Expert/SELC Education	Training material for government employees to promote the understanding and application of the DHS SELC, and support the DHS Program/Project Management Training Program.	As required
2	Process Improvement Documentation	Subject Matter Expert/Process Improvement Support	Processes and procedures to be used by the office to bring their projects into compliance with DHS and OIT requirements.	As required
3	Status Reports	All	At a minimum, status update briefings shall be presented to the Executive Lead on a weekly basis at regular team meetings. If conditions warrant, ad hoc reports may be requested on a more frequent basis. Status updates shall include information on processes and procedures being drafted and implemented.	At minimum, weekly at regular team meetings
4	User Training	Subject Matter Expert/SELC Education	Materials shall be developed and training sessions shall be presented to ELCM Tool Suite users.	As required
5	Briefings to OIT Management and Stakeholders	All	As required, short briefings shall be prepared and presented to OIT Management and ELCM/PAL stakeholders.	As required

6.3 Dependencies

If the dependencies on other CBP activities and/or personnel impact a due date assigned to any deliverable or work product, CBP shall work with Contractor to appropriately adjust the affected delivery date(s) based on the resolution of those dependencies and/or availability of personnel.

6.4 Review

Unless otherwise defined in writing from the Executive Lead, deliverables will undergo the formal review and acceptance process as defined in the OIT-level Document Deliverable Review Process. The work products and artifacts identified in this contract shall be reviewed within the appropriate working group and by the appropriate Government stakeholders. Any revisions as a result of these reviews shall be incorporated into the work product or artifact prior to delivery. The Contractor shall work with CBP to determine the review cycle for the final approval dates. The Contractor shall provide a schedule of all deliverable reviews, showing dates that deliverables will be distributed. The schedule shall allow at least three (3) days for review of distributed materials prior to a meeting; exceptions to this schedule to be mutually agreed upon.

6.5 Delivery Methods

All deliverables and associated documents will be submitted to CBP via secure e-mail in electronic form and stored in designated shared network drives. Documents shall not be transmitted outside of cbp.gov. All standard documents will be produced in standard Microsoft Office or Adobe PDF formats.

6.6 Formats

Documents will be submitted in at least one of the following formats:

- Document – Microsoft Word, Microsoft PowerPoint or Adobe PDF document that represents a stand-alone report.
- Briefing – Microsoft PowerPoint or Adobe PDF presentation.
- Facilitation – Materials and meeting leadership to direct the deliberations of a group towards a pre-specified objective.
- Web – Series of linked HTML or comparable web pages and data bases that provides the reader with a set of web pages accessible through a browser.

6.7 Performance Standards

Table 2, *Performance Standards*, shown below reflects the performance standards that have been established by the Government. This table also indicates the areas in which are most important for the successful performance of this effort.

All performance objectives shall be tracked each month to get an overall total measurement.

Program Service Objective	Required Service	Surveillance Methodology	Performance Standard
RESPONSIVENESS	Applicable to All	Daily Interactions with OIT Personnel	**Outstanding**: Totally responsive, flexible, and proactive to changes in direction and adapting resources to successfully deal with the changes. Project organization consistently assures on time or early responses to all deadlines. No adverse effect on productivity, performance or delivery. **Excellent:** Very responsive and flexible to changes in direction and adapting resources to successfully deal with the changes. Project organization assures on time responses to short fuse deadlines in almost all cases. Rarely is there an adverse effect on productivity, performance or delivery. **Satisfactory**: Met contract requirements. Adjusts easily to changes on many occasions. Little adverse effect on productivity, performance, or delivery. **Marginal:** Met contract requirements, generally. Occasional delays or difficulty in meeting suspense. Overall responsiveness could be improved. **Unsatisfactory**: Has not met contract requirements.
COMPLIANCE WITH MILESTONES/ DELIVERABLES	Applicable to All	Daily Interactions with OIT Personnel	**Outstanding:** Impeccable record in meeting milestone/due dates, all of which are completed early, unless otherwise directed by CBP. **Excellent**: Exemplary record in meeting milestone/due dates, many (the majority) of which are completed early. **Satisfactory:** Met requirements. Schedule problems are usually identified in time for corrective action; milestones/due dates are almost always achieved and instances where they are not are of minor impact. **Marginal:** Met contract requirements generally, but some work may be late or need to be redone. **Unsatisfactory**: Has not met contract requirements.

Program Service Objective	Required Service	Surveillance Methodology	Performance Standard
CONTRACT MANAGEMENT, REPORTING, AND SUPERVISION OF RESOURCES	Applicable to All	Daily Interactions with OIT Personnel	**Outstanding:** Provides extraordinarily motivated, competent, and professional personnel. Positive attitudes. Strong teamwork. Personnel need virtually no supervision and are highly proficient in their work. The contractor anticipates and plans for problem areas. Minimal personnel turnover. Resources are replaced, when necessary, without impacting workload or mission activities. **Excellent:** Highly talented workforce that is motivated and displays more times than not successful teamwork. Personnel are competent and training is provided to upgrade or improve skills. Reports are of high quality and completeness. Efficient recruitment and personnel management. Supervision ensures quality performance, teamwork, and work efficiency. **Satisfactory:** Met requirements. Communicative and capable management. Oversees activities in a very competent and professional manner. Direction of subcontractors or consultants meets and in some instances exceeds all requirements of the contract. Reports are thorough, accurate, self-explanatory and meet the CBP Program Offices' expectations. **Marginal:** Generally met contract requirement, but occasional delays or mission impact occurs due to lack of communication, proficiency, high turnover, delays in replacing personnel or lack of supervision. Reports do not always meet expectations. **Unsatisfactory**: Has not met contract requirements.

Program Service Objective	Required Service	Surveillance Methodology	Performance Standard
QUALITY	Applicable to All	Daily Interactions with OIT Personnel	**Outstanding:** Deliverables, services, or other performance output always exceed CBP Program Offices' needs and expectations and/or the acceptable quality levels identified in the Quality Assurance Plan . Quality consistently exceeds an acceptable level, in a way that is of great importance to CBP. Contractor is extremely dependable; work/products almost always exceed contract requirements or specifications. Contractor never delivers inaccurate, or unsatisfactory goods or services, contractor demonstrates very high level of dedication and ability. Provides innovative solutions. **Excellent:** Deliverables, services, or other performance output almost always exceed CBP Program Offices' needs or expectations and/or the acceptable quality levels identified in the Quality Assurance Plan. Quality usually exceeds an acceptable level to a significant degree, contractor is highly dependable, work/products frequently exceed contract requirements or specifications. Contractor never delivers inaccurate or unsatisfactory goods or services. Highly professional products. **Satisfactory:** Met requirements. Deliverables, services, or other performance output meet and sometimes exceed needs and expectations and/or the acceptable quality levels identified in the Quality Assurance Plan, output is often dependable, work is completed according to contract requirements and specifications and sometimes exceeds it. Output contains few, if any, non-conformances. Areas of inaccurate work or unsatisfactory results are minor and do not have a significant adverse impact on CBP's mission. **Marginal:** Met contract requirements generally, but some lack the professional work that CBP expects **Unsatisfactory**: Has not met contract requirements.

Program Service Objective	Required Service	Surveillance Methodology	Performance Standard
COST MANAGEMENT AND LABOR HOUR EFFICIENCY	Applicable to All	Daily Interactions with OIT Personnel	**Outstanding:** Cost controls are highly effective and consistently result in considerable savings. Costs are always below estimates and there are no cost overruns unless directed by CBP due to factors beyond contractor control. **Additionally, it can be proven that the contractor has been able to affect substantially lower development and maintenance costs by reducing software redundancies or other asset reuse.** Labor Hour variances by labor category show exceptional management of labor mix and delivery of agreed skill sets. Variances are explained in a manner that shows benefit to the Government. Price requests for award terms, if applicable, are submitted with extremely clear documentation. **Excellent:** Cost controls are highly effective and result in considerable savings on occasion. Costs are usually below estimates, and there are no cost overruns unless directed by CBP due to factors beyond contractor control. Additionally, it can be proven that the contractor has been able to affect lower development and maintenance costs by reducing software redundancies or other asset reuse. Labor hour variances by labor category show effective management of labor mix and delivery of hours. Variances are effectively managed and explained. Documentation for pricing award terms, if applicable, are submitted without errors or omissions. **Satisfactory:** Costs are in accordance with estimates and there are no cost overruns, unless directed by CBP due to factors beyond contractor control. There are initiatives and tools in place to facilitate cost control. The contractor can substantiate some lower development and maintenance costs due to the reductions in software redundancies or other asset reuse. Labor hour variances show delivery of labor hours and skill sets in accordance with the agreed labor, qualifications and rates matrix. Documentation for pricing in award term, if applicable, adequately supports the request(s) without requests for clarification and follow-up. **Marginal:** Met contract requirements, generally but it appears some projects could have been performed more efficiently with fewer labor hours or lower scaled labor categories. No or poor documentation showing a reduction in software redundancies or other asset reuse. Labor hour variances include many negative variances that are inadequately explained and that show a considerable lack of control of labor mix or neglect in meeting the requirements of the agreed labor, qualification, and rates matrix. **Unsatisfactory:** Has not met contract requirements.

7.0 Government Furnished Equipment and Materials

7.1 Government Furnished Equipment

As provided for in Section H.8(a) of the EAGLE Contract, each person covered under this contract will be provided the following by the CBP Office of Information and Technology:

- A standard-sized working area (cube)
- A personal computer (PC) with CBP standard desktop applications
- Standard PC input devices and peripherals, i.e., a mouse, a keyboard, a monitor
- A connection to the OIT Local Area Network (LAN)
- A connection to an OIT LAN printer.
- A Mobi-key to permit telecommuting as established in Section 14.2 below.

7.2 Government Furnished Materials

As provided for in Section H.8 (b) of the EAGLE contract, the Government shall provide current versions (which may be in draft format) of all requisite information and materials necessary to conduct the work described in this Statement of Work. The Contractor shall aid in the identification of requisition information and materials and provide the request at least 30 days in advance of requested delivery.

8.0 Contractor Furnished Materials and ODCs

Proprietary tools/applications shall not be used without prior CBP approval. All tools/applications shall be compliant with CBP Enterprise Architecture. If any proprietary tools are used, the Contractor shall furnish sufficient copies of all tools and documentation and provide a license for unlimited rights to use by CBP and its duly appointed agents.

9.0 Accessibility Requirements (Section 508 Compliance)

9.1 Accessibility Requirements (Section 508)

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

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

9.2 Section 508 Applicable EIT Accessibility Standards

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

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

36 CFR 1194.24 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 1194.31 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.

9.3 Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

9.4 Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets

less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

10.0 Enterprise Architecture (EA) Compliance

When applicable, the Offeror shall ensure that the design conforms to the DHS Homeland Security (HLS) and CBP EA, and all DHS and CBP policies and guidelines as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA) such as the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture Technical Framework.

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

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

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

When applicable, description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model (DRM) and Enterprise Architecture Information Repository. Submittal shall be through the CBP Data Engineering Branch (DEB) and CBP Enterprise Architecture Branch (EAB).

When applicable, all developed solutions shall be compliant with the HLS and CBP EA.

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

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

11.0 ISO (Information Security) Compliance

11.1 General Information Security Clause

"All services provided under this task order must be compliant with DHS Information Security Policy, identified in MD4300.1, *Information Technology Systems Security Program* and *4300A Sensitive Systems Handbook*."

11.2 Interconnection Security Agreements

If applicable, 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 Authorizing Officials (AOs) or by the official designated by the AO to have signatory authority.

11.3 3052.204-70 Security Requirements For Unclassified Information And Technology Resources (JUN 2006)

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

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

(1) If applicable, within 120 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) If applicable, the Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et

seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

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

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

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

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

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) If applicable, within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 8.0, March 14, 2011) 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.

11.4 CONTRACTOR EMPLOYEE ACCESS (JUN 2006)

3052.204-71 Contractor employee access.

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

HSAR 3052.204-71 Contractor Employee Access Clause

The chart below shows how to apply HSAR 3052.204-71 Contractor Employee Access to Acquisition Documents. The clause and its alternates follow.

Task requires recurring access to Government facilities or access to sensitive information	Basic Clause

Requires access to IT resources	Basic Clause + Alternate I
No IT access, but access to sensitive information is limited to U.S. Citizens & lawful permanent residents	Basic Clause + Alternate II

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

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

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

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

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

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

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT

resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

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

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

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

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

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR 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 COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

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

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

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

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

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

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

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

11.5 Security Certification/Accreditation

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with the current version of the DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05, and all applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series). During all SELC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools. An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, the System Owner is always responsible for information system security (4300A). System owners shall include information security requirements in their capital planning and investment control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS information system. System owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

11.6 Disaster Recovery Planning & Testing – Hardware

If applicable and if the system owner requires a robust DR solution (full redundancy and failover capabilities (for near zero downtime)) then the funded DR solution must match the production environment like-for-like. This solution would also include additional software licenses, hardware, firmware and storage for the DR environment.
If applicable, the system owner or program office must also include travel, per diem and approximately 16 over the core hours for travel to recovery facilities twice per fiscal year for system administrators, DBA's, end users or testers

If applicable and if the system owner requires a moderate DR solution that would provide a working environment that is capable of handling their mission essential functions then they can fund a scaled down solution which should still take into consideration additional hardware, software licenses, and storage for the DR environment.

If applicable, the system owner or program office is still responsible for the costs associated with testing their DR solution; however, for a scaled down solution, it may be possible to leverage or share staff already designated to participate in DR activities.

If applicable, and if the system owner only requires a low DR solution then the system owner or program office can use internal resources to perform a table-top exercise, which generally does not require travel, additional hardware or software licenses.

11.7 Security Review and Reporting

(a) The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, Office of Inspector General, the CBP Chief Information Security Officer, authorized Contracting Officer's Representative (COR), and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

11.8 Access to Unclassified Facilities, Information and Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information and 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.

11.9 OMB-M-07-18 FDCC

In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at

http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.

11.10 Personal Identification Verification (PIV) Credential Compliance

If and when applicable, the custom software product being developed must be enabled to use PIV credential for authentication purposes, in accordance with NIST guidelines including Federal Information Processing Standard Publication (FIPS) 201 (Demonstrated progress toward integration with AppAuth would be considered a confirmation to PIV enablement).

Authorities for this requirement are as follows:

- HSPD-12 —*Policies for a Common Identification Standard for Federal Employees and Contractors*
- OMB M-11-11 —*"Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"*
- OMB M-06-16 —*Acquisition of Products and Services for Implementation of HSPD-12*
- NIST FIPS 201 —*Personal Identity Verification (PIV) of Federal Employees and Contractors*
- NIST SP 800-63 —*Electronic Authentication Guideline*
- OMB M-10-15 —*FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors. 9 IT AR Quick Essentials Guide 2011 v2.0

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

11.11 Encryption Compliance

If encryption is required, the following methods are acceptable for encrypting sensitive information:

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
2. National Security Agency (NSA) Type 2 or Type 1 encryption.
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A), for Sensitive Systems).

12.0 Contractor Signature Format

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

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

[Name]
(Contractor)
[Position or Professional Title]
[Company Name]
Supporting the XXX Division/Office...
U.S. Customs & Border Protection
[Phone]
[FAX]

13.0 Period of Performance

Periods of performance will twelve months long as detailed below.

Contract Period	Start Date	End Date
Base Period	8/1/2009	7/31/2010
Option Period 1	8/1/2010	7/31/2011
Option Period 2	8/1/2011	7/31/2012
Option Period 3	8/1/2012	7/31/2013
Option Period 4	8/1/2013	7/31/2014

Options may be exercised based on the availability of funding and continuing need.

14.0 Place and Hours of Performance

14.1 CBP Locations

(a) U.S. Customs and Border Protection (CBP) will provide limited space in multiple facilities for the on-site contractor staff to perform the required tasks.

(b) Performance will take place at various CBP offices, the Recovery Point Services Facility in Gaithersburg, MD, and EOTE Integration Laboratory, and Enterprise Test laboratories, most of which are located within a 50 mile radius of Washington, DC. Space at these facilities is limited. The contractor will be provided access to a high speed printer at each site and will be furnished with a desk and office supplies (i.e., desk, chairs, phones, etc). No other office equipment will be supplied.

14.2 Telecommuting

Telecommuting is permitted under the contract provided the following guidelines are strictly adhered to.

14.2.1 Approval to Telecommute

Contractor telecommuting will be approved by the COR on a case by case basis, and may not be overused/abused.

14.2.2 Equipment to Be Used

Remote access is permitted only with Government supplied connection devices, such as a MOBIKEY.

14.2.3 Primacy of the Traditional Worksite

Contract employees who telecommute must be available to work at the traditional worksite if necessitated by work requirements. The traditional worksite is the contractor employee's primary work location, and as such use of alternative worksites may not be a substitution for the requirement to work at the traditional worksite. Time spent in a telecommuting status must be accounted for and reported in the same manner as if the employee reported for work at the traditional worksite. The contractor employee is required to satisfactorily complete all assigned work, consistent with the contract's requirements. Furthermore, the contractor employee must work overtime only when ordered and approved by the government [CO and COR] in advance.

14.2.4 Classified Documents

No classified documents (hard copy or electronic) may be taken to an employee's alternative worksite. During telecommuting sessions, sensitive unclassified material, including Privacy Act and For Official Use Only data, may only be used by contractor employee provided with Government-furnished equipment. The contractor employee is responsible for the security of all official data, protection of any Government-furnished equipment/information, and carrying out the contract requirements at the alternative worksite.

14.2.5 Government Liability

The Government is not liable for damages to a contractor employee's personal or real property or to others' property while the contractor employee is working at the approved alternative worksite.

14.3 Work Hours

Contractor shall typically work 8 hours a day, 5 days a week, but may be required to work beyond this typical schedule with the proper authorization as set forth by the COR. Contractor personnel shall observe a consistent tour of duty of 40 hours per week. Any alterations to the work schedule shall be approved by the COR. Contractor personnel shall be available for weekend and after hours work as directed by the COR, and may be called upon for after-hours emergencies. Unless otherwise agreed upon with the COR, all Contractor personnel shall be present during core hours and have the appropriate skill sets to support the services in this SOW. Core hours are 9AM to 3PM.

14.4 Overtime

As specified in the FAR, Section 52.222-2 Payment for Overtime Premiums. Payment for Overtime Premiums (July 1990)

(a) The use of overtime is authorized under this contract if the overtime premium does not exceed zero (0) or the overtime premium is paid for work—

(1) Necessary to cope with emergencies such as those resulting from accidents, natural disasters, breakdowns of production equipment, or occasional production bottlenecks of a sporadic nature;
(2) By indirect-labor employees such as those performing duties in connection with administration, protection, transportation, maintenance, standby plant protection, operation of utilities, or accounting;
(3) To perform tests, industrial processes, laboratory procedures, loading or unloading of transportation conveyances, and operations in flight or afloat that are continuous in nature and cannot reasonably be interrupted or completed otherwise; or
(4) That will result in lower overall costs to the Government.

(b) Any request for estimated overtime premiums that exceeds the amount specified above shall include all estimated overtime for contract completion and shall—

(1) Identify the work unit; *e.g.*, department or section in which the requested overtime will be used, together with present workload, staffing, and other data of the affected unit sufficient to permit the Contracting Officer to evaluate the necessity for the overtime.

14.5 Observance of Legal Holidays and Excused Absence

All provisions of Section H.25 of the EAGLE contract are hereby incorporated by reference.

15.0 Travel and Other Direct Costs

See EAGLE Contract Sections H.5, Contractor Justification for Other Direct Costs (ODCs) and H.6, Selection Items of Costs

16.0 Billing and Invoices

16.1 Invoice Content

All invoices submitted under this contract shall include, at a minimum:

- The Invoice Number
- The Contract and/or Task Order Number
- A detailed breakdown by employee of the total number of hours worked
- The full, loaded hourly rate charged
- A description of the work accomplished during the billing period
- The vendor's tax identification number
- Signature of the Vendor's authorized personnel

16.2 Invoicing Submission and Deadlines

Invoices shall be submitted to the CBP National Finance Center with electronic copies to the Contracting Officer's Representatives listed in Section 19.2.

Invoices for hours worked in a given month shall be submitted to the National Finance Center and the COR by the 20th day of the following month. For example, an invoice for hours worked in May 2009 shall be submitted to the CBP National Finance Center and the COR no later than the 20th day of June 2009.

17.0 Government Contacts

17.1 Executive Lead

Name: (b) (6)
Telephone Number: (703) (b) (6)
Email: (b) (6) @dhs.gov

17.2 Contracting Officer's Representative (COR)

Name: (b) (6)
Telephone Number: (703) (b) (6)
Email: (b) (6) @dhs.gov

17.3 Alternate COR

Name: (b) (6)
Telephone Number: (703) (b) (6)
Email: (b) (6) @dhs.gov

Appendix A: Acronyms

Acronym	Meaning
BI	Background Investigation
BPR	Business Process Re-engineering
CBP	U.S. Customs and Border Protection
CBT	Computer Based Training
CFR	Code of Federal Regulations
COR	Contracting Officer's Representative
COTS	Commercial-Off-the-Shelf
DDC	CIT Deputy Directors' Council
DHS	Department of Homeland Security
EA	Enterprise Architecture
EARB	Enterprise Architecture Review Board
EDME	Enterprise Data Management and Engineering Division.
EDMO	DHS Enterprise Data Management Office
EIT	Electronic Information Technology
ELCM	Enterprise Life Cycle Methodology
FAR	Federal Acquisition Regulations
FTE	Full Time Equivalent
GFE	Government-Furnished Equipment
GOTS	Government-Off-the-Shelf
HLS	Homeland Security
IT	Information and Technology
MD	Management Directive
OA	CBP Office of Administration (formerly Office of Finance)
OAST	DHS Office on Accessible Systems and Technology
OIT	Office of Information and Technology
OMB	Office of Management and the Budget
OTIA	Office of Technology Innovation and Acquisition
PAL	Process Asset Library
PCII	Protected Critical Infrastructure Information
PMB	Process Management Branch
PTR(s)	Problem Trouble Reports
SELC	Systems Engineering Life Cycle
SOW	Statement of Work
SSI	Sensitive Security Information
TO	Task Order
U.S.C.	United States Code
WBS	Work Breakdown Structure