ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 2

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

1. DATE OF ORDER: 08/01/2009
2. CONTRACT NO. (if any): HSHQDC06D00018
3. ORDER NO.: HSBP1009J27216
4. REQUISITION/REFERENCE NO.: 0020044414
5. ISSUING OFFICE (Address correspondence to):
Department of Homeland Security
Customs & Border Protection
1300 Pennsylvania Ave., NW
NP 1310
Washington DC 20229

6. SHIP TO:
a. NAME OF CONSIGNEE
See Attached Delivery Schedule
b. STREET ADDRESS
c. CITY | d. STATE | e. ZIP CODE
f. SHIP VIA

7. TO:
a. NAME OF CONTRACTOR
LOCKHEED MARTIN MISSION
b. COMPANY NAME
SYSTEMS
c. STREET ADDRESS
700 N FREDERICK AVE
d. CITY: GAITHERSBURG | e. STATE: MD | f. ZIP CODE: 20879-3328

8. TYPE OF ORDER
☐ a. PURCHASE - Reference Your _____
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
☒ b. DELIVERY - Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA

10. REQUISITIONING OFFICE
(b) (6)

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
☐ a. SMALL ☒ b. OTHER THAN SMALL
☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED
☐ e. HUBZone ☐ f. EMERGING SMALL BUSINESS
☐ g. SERVICE-DISABLED VETERAN-OWNED

CONTRACTOR TIN: (b) (3); (b) (4)

12. F.O.B. POINT: Destination

13. PLACE OF: a. INSPECTION | b. ACCEPTANCE

14. GOVERNMENT B/L NO.

15. DELIVER TO F.O.B POINT ON OR BEFORE (Date): 07/16/2010

16. DISCOUNT TERMS: NET 30

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QTY Accpt (g)
00010	ELCM/PAL Support	1.00	AU	$1,353,837.00	$1,353,837.00	

18. SHIPPING POINT | 19. GROSS SHIPPING WEIGHT | 20. INVOICE NO.

17(h) TOT. (Cont. pages): $0.00

21. MAIL INVOICE TO:
SEE BILLING INSTRUCTIONS ON REVERSE
a. NAME: DHS - Customs & Border Protection National Finance Center
b. STREET ADDRESS (or P.O. Box): P.O. Box 68908
c. CITY: Indianapolis | d. STATE: IN | e. ZIP CODE: 46268

17(i) GRAND TOTAL: $1,353,837.00

22. UNITE BY (Signa (b) (6)

23. NAME (Typed)
Stephon Doswell
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

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

Federal Tax Exempt ID: 72-0408780

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

NOTES:

This labor hour type task order is issued against DHS's Enterprise Acquisition Gateway for Leading-Edge Solutions (EAGLE) contract, contract number HSHQDC-06-D-00018. All terms and conditions of both the EAGLE contract and this task order are in full effect.

This task order is issued for Enterprise Life Cycle Methodology and Process Asset Library Support Services for the CBP Enterprise Data Management & Engineering Division (EDME), in accordance with the attached Statement of Work (SOW) and Lockheed Martin Corporation Information Systems & Global Services proposal dated May 26, 2009.

The SOW and Price Proposal are hereby incorporated into this task order.

The period of performance of this order is as follows:
Base Period: 08/01/09 - 07/31/10
Estimated Ceiling Amount: $1,353,837.00
Option Period 1: 08/01/10 - 07/31/11
Estimated Ceiling Amount: (b) (4)
Option Period 2: 08/01/11 - 07/31/12
Estimated Ceiling Amount: (b) (4)
Option Period 3: 08/01/12 - 07/31/13
Estimated Ceiling Amount: (b) (4)
Option Period 4: 08/01/13 - 07/31/14
Estimated Ceiling Amount: (b) (4)

All labor rates are fixed unit prices.

The total not to exceed (NTE) ceiling amount for this task order is (b) (4) (Base Period plus 4 Option Periods).

(b) (6) is the designated Contracting Officer's Technical Representative(COTR) for this Task Order.

Please submit all invoices to each of the following:

EDME Budget Team
7501 Boston Blvd., Room 211
Springfield, VA 20598

Attn: (b) (6)
7501 Boston Boulevard, NDC-2, (b) (6)
Springfield, VA 22153

Reference: Lockheed Martin Corporation Information Systems & Global Services proposal dated May 26, 2009 and the Statement of Work (SOW).

ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: HSBP1009J27216

SCHEDULE OF SUPPLIES/SERVICES

Item Number: 00010 **Line Item (Priced/Information/Option):** P
Supplies/Services: ELCM/PAL Support

Qty	Unit	Unit Price	Ext. Price
1	AU	$1,353,837.0000	$1,353,837.0000

Total Funded Contract Value: **$1,353,837.00**

ELCM/PAL -- Enterprise Life Cycle Methodology and Process Asset Library Support Statement of Work

January 16, 2009

Table of Contents

1.0 Overview 1

2.0 Scope of Work 1

3.0 General Requirements and Background Information 1

4.0 Expectations and Assumptions 2

5.0 Key Personnel 3
5.1. Work Hours 3
5.2 Overtime 4

6.0 Labor Category Functions 4

6.1 Information Technology Senior Consultant/Team Lead 4
6.2 Information Technology Senior Consultant 4
6.3 Information Technology Senior Consultant/Project Manager 5
6.4 Information Technology Consultants 5
6.5 Business Process Reengineering Specialist/ELCM-PAL Librarian 5

7.0 Deliverables and Delivery Schedule 6

8.0 Performance Measures and Acceptance Criteria 8

8.1 Performance Measures 8
8.2 General Acceptance Criteria 9

9 9

.0 Government Furnished Equipment and Materials 9

9.1 Government Furnished Equipment 9
9 10
.2 Government Furnished Materials 10

10.0 Contractor Furnished Materials and ODCs 10

11.0 Section 508 Requirements 10

11.1 36 CFR 1194.21 – Software Applications and Operating Systems 10
11.2 36 CFR 1194.22 –Web-Based and Internet Information Applications 11

12.0 Enterprise Architecture Requirements 12

13.0 Security Requirements 12

13.1 Security Requirements for Unclassified Information Technology Resources 12
13.2 Contractor Employee Access 13
13.3 Security Certification/Accreditation 15
13.4 Security Review and Reporting 15
13.5 Security Procedures 16

14.0 Contractor Signature Format 18

15.0 Period of Performance 18

Table 5. Base and Option Periods of Performance 18

16.0 Place of Performance 18

16.1 Location 18
16.2 Other Locations Where Work May be Required 19
16.3 Telecommuting 19
17.0 Travel and Other Direct Costs 19

18.0 Billing and Invoices 20

18.1 Invoice Content 20
18.2 Invoicing Submission and Deadlines 20

19.0 Government Contacts 20

19.1 Executive Leads 20
19.2 Contracting Officer's Technical Representative (COTR): 21

Appdenix A Acronyms A-1

1.0 Overview

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 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 Library (PAL), and the Online CBP and DHS System Life Cycle (SLC) to integrate all OIT 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 and process improvement services to operate and maintain the OIT ELCM Tool Suite consisting of the ELCM, the Online CBP and DHS SLC, and the OIT PAL.

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 perform operational and maintenance support of the complex OIT ELCM Tool Suite. There are seven (7) aspects to the services required:

a. The administration of process management implementation;
b. Continued development, programming, and enhancement of the OIT ELCM Tool Suite.
c. Support CBP OIT implementation of the PAL Tool
d. Support the CBP Office of Finance (OF) implementation of the PAL tool.
e. Integrating OIT, CBP, and DHS SLC implementations
f. Mentoring and training ELCM Tool Suite Users
g. Assisting in development of process assets.

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, Earned Value Management (EVM) policy 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), Information Technology Infrastructure Library (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), Architecture Review Board (ARB) and Deputy Directors' Council (DDC) priorities, painpoints, strategies and opportunities. ELCM staff shall also address Problem Trouble Reports (PTRs) and develop ELCM Tool Suite enhancements. Enhancements shall be focused on supporting OIT Process Integration, SLC Project/Program Support (tailoring, status, link to project artifacts), and enhanced process flow display. Other enhancements shall address project views and ELCM pilot feedback. Additionally, the Contractor shall be required to:

a. Manage and Execute ELCM Tool Suite Changes
b. Analyze Changes and Update ELCM Tool Suite processes
c. Develop Formal ELCM Tool Suite Training
d. Implement Formal ELCM Tool Suite Training
e. Update ELCM Computer Based Training (CBT) and Orientation Training
f. Analyze ELCM Processes
g. Perform ELCM Gap Analysis

The Contractor shall also mentor and support CBP's Office of Finance (OF) personnel in their implementation of the OF PAL.

DHS components are consolidating their data centers to two (2) DHS Enterprise Data Centers. CBP plans to migrate ELCM, PAL, and Online CBP production systems to DHS Enterprise Data Centers. The Contractor shall continue to meet the requirements of this Statement of Work (SOW) regardless of the location of the production environment.

4.0 Expectations and Assumptions

(a) Acceptance of a deliverable or work product occurs when the OIT Process Management Branch Chief accepts via written notification sent to the Contractor. Contractor shall then work with the Process Management Branch to obtain the appropriate management approvals for deployment to the organization.

(b) Contractor shall manage the task within cost, continue efforts to optimize the application, resolve ELCM Tool Suite Problem Tracking Reports (PTR) and participate in process engineering and integration efforts to support the closing of ELCM gaps identified in the Gap Analysis.

(c) In addition, the Contractor shall place emphasis on

- Integrating with ongoing SLC activities at the OIT, CBP and DHS levels

- Integrating with ongoing project management discipline implementation, education, and deployment.`
- Training and mentoring key users on OIT ELCM Tool Suite
- Training and mentoring OF personnel on the PAL tool
- Providing Project/Program support (e.g. tailoring, status, link to project artifacts),
- Providing requirements for and executing enhancements/modifications to the ELCM Tool Suite
- Providing requirements for and executing enhancement/modifications to the OF PAL tool implementation; and
- Ensuring Enterprise processes are mapped to the OIT ELCM Tool Suite.

5.0 Key Personnel

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

Table 1 Key Personnel

EAGLE Labor Category	Level	Number of Positions
(b) (4)	(b) (4)	(b) (4)

- The key personnel specified in Section 5.0 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 Technical Representative (COTR) 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 COTR, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action in order to enable the COTR to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel until the COTR approves the change.

5.1 Work Hours

Contractor shall typically work 8 hours a day, 5 days a week, but may be required to work beyond this typical schedule. 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 COTR. Contractor personnel shall be available for weekend and after hours work as directed by the COTR, and may be called upon for after-hours emergencies. 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.

5.2 Overtime

Contractor personnel shall not work more than forty (40) hours a week without prior approval from the Contractor's Program Manager and COTR.

6.0 Labor Category Functions

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

6.1 Information Technology Senior Consultant/Team Lead

- Prepare an Operations/Project Plan (including a Work Break Down Structure) covering the tasks to be performed in support of the OIT ELCM Tool Suite.
- Manage OIT ELCM Tool Suite total life cycle software development
- Perform OIT ELCM Tool Suite software configuration and change management, including participation in configuration control boards, processing change requests in Dimensions, and coordinating with technical support organizations.
- Prepare and analyze technical requirements, including recommended software and hardware specifications
- Integrate DHS, CBP and OIT strategic priorities into a Requirements Traceability Matrix.
- Prioritize OIT ELCM Tool Suite system integration, system maintenance and sustaining engineering for development, testing, and production environments
- Perform OIT ELCM Tool Suite problem resolution including system troubleshooting and requirements and software analysis throughout the system life cycle.
- Perform System, Unit and Integration Testing
- Manage OIT ELCM Tool Suite software engineers in their support of both the OIT ELCM Tool Suite and the OF implementation of FuturePoint™
- Report status of enhancements, PTR resolutions to Executive Lead and the COTR on a regular basis.

6.2 Information Technology Senior Consultant

- 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, painpoints, 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
- Test enhancements and problem ticket solutions to ensure that they meet the required objective before the new code is submitted for formal system acceptance testing.

- Provide expert consultation services to senior OIT management in identifying key process areas that need to be addressed.
- Mentor key ELCM Tool Suite users.

6.3 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 COTR as required
- Identify replacements in the event contractor must be replaced

6.4 Information Technology Consultants

- Perform OIT ELCM Tool Suite and OF 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
CSS	

- Perform ELCM Tool Suite and OF PAL problem resolution including system troubleshooting
- Perform requirements and software analysis throughout the system life cycle.
- Perform ELCM Tool Suite and OF PAL 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.

6.5 Business Process Reengineering Specialist/ELCM-PAL Librarian

- Catalog all submission 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.

- Work with submitters to remedy any deviations from OIT standard formats and templates.
- Support ELCM Suite vision and mission.

7.0 Deliverables and Delivery Schedule

A table of deliverables that summarizes the minimum set of deliverables required under this task order is found in Table 2 below. The draft and interim deliverables shall be in the formats or modes in Table 2. The Contractor may propose other products deemed necessary or appropriate. Documents are to be delivered in accordance with the terms of this SOW as well as any additional instructions in the delivery/task order.

Unless otherwise defined in writing from the CBP Executive Lead, deliverables shall undergo the formal review, testing, and acceptance process as defined by OIT 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 prior to delivery. The Contractor shall work with CBP to determine the review cycle and the final approval dates. The Contractor shall provide a schedule of all deliverable reviews, showing dates that deliverables shall be distributed. The schedule shall allow at least three (3) days for review of distributed materials prior to a meeting. Exceptions to this schedule shall be mutually agreed upon.

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

All final deliverables shall be under OIT Configuration Management (CM) and published to the Modernization Program web portal or OIT Process Asset Library (PAL) as directed by the CBP Executive Lead. The Contractor shall update work products posted on the Web Portal/OIT PAL as required. The Contractor shall then post the updates to the Web Portal/OIT PAL.

Documents shall be submitted in several formats:

- Document – Microsoft Word, Microsoft PowerPoint, or Adobe PDF document that represents a stand-alone report. MS Excel may also be used for numerical data if appropriate.
- Briefing – Microsoft PowerPoint or Adobe PDF presentation.
- 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

Table 4 summarizes the minimal set of work elements required under this task and the respective type and delivery date for the final product. Documents are to be delivered in general accordance with the terms of this task statement.

Table 3. Deliverables

No.	Deliverable	Description	Due Date
1	Operations/Project Plan (Including WBS)	Document the operational methods, processes and procedures. Include a WBS that shall be used to track progress.	Within 30 days of contract award
2	Statements of Requirements	Document changes to requirements generated by enhancements or changing Federal regulations. This includes technical requirements including recommended software and hardware specifications.	As required
3	Schedule of Enhancements	There are enhancements pending to the ELCM Roadmap. The Contractor shall update this schedule as necessary with the concurrence of CBP.	As required
4	PTR Responses	Document PTRs and their solutions. See Section 8.1 below.	As required
5	Change Requests	Document change requests in Dimensions for consideration by the appropriate Change Control Boards. See Section 8.1 below.	As required
6	Test Reports	Document the results of System, Unit and Integration Testing	Within 10 days of each System, Unit, and Integration Test
7	Enhancements to fit COTS PAL tool.	As the PAL tool evolves, changes may be required to the ELCM Tool Suite and the OF implementation. The nature of these required changes and the programming solutions shall be documented.	As required
8	Enhancements/Changes required by law or DHS	From time to time, changes in law and DHS regulations require changes to the ELCM Tool Suite. The nature of the changes required and the programming solutions shall be documented	As required

No.	Deliverable	Description	Due Date
9	Gap Analysis	Document gaps and overlaps in existing Enterprise process assets. This shall assist OIT senior management in identifying key process areas that need to be addressed. See Section 8.1 below	As required
10	Status Reports	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.	At minimum, weekly at regular team meetings
11	User Training	Materials shall be developed and training sessions shall be presented to ELCM Tool Suite users.	As required
12	Requirements Traceability Matrix	Continuously documents requirements flowing from DHS, CBP, and OIT. Prioritizes and assign these requirements to releases.	As required
13	Briefings to OIT Management and Stakeholders	As required, short briefings shall be prepared and presented to OIT Management and ELCM/PAL stakeholders.	As required

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.

8.0 Performance Measures and Acceptance Criteria

8.1 Performance Measures

PM1. The contractor shall provide performance and outcome measures of success as follows:

a. Number of CIO, ARB, and DDC Process Baseline strategic priorities (1) identified and (2) closed (quarterly)
b. Measures of DHS, CBP, and OIT strategic and tactical priorities aligned to and incorporated into, the ELCM Tool Suite (quarterly)
c. Number of OIT Process Assets in Process Baseline (monthly)
d. Number of new practice gaps identified (monthly)
e. Number of practice gaps closed (monthly)

f. Number of PTRs closed (quarterly)
g. Number of Change Requests (CRs) closed (quarterly)

PM2. The Contractor shall follow the OIT issues and risk resolution process for all issues and risks identified/accepted as appropriate by the CBP Team Lead. The Contractor shall enter the issue into the issues database within 48 hours of concurrence by CBP Executive Lead.

PM3. The Contractor shall produce a series of reports, including the reports listed above as items PM1 (a – g), with the content and format specified by CBP. Reports include the following:

a. Weekly status report (includes progress against milestones, issues, resolutions, escalations, projections)
b. Labor report (includes planned vs. actual FTE hours)
c. Project Plan in Microsoft Project software
d. Meeting minutes (includes action items)

PM4. Deliverables and work products must be complete, delivered on time per the Project Plan with no outstanding issues at time of delivery.

8.2 General Acceptance Criteria

The general quality measures, as set forth below shall be applied to each work product received from the Contractor under this contract.

Accuracy - Work products shall be accurate in presentation, technical content, and adherence to accepted elements of style.

Clarity - Work products shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand and relevant to the supporting narrative.

Specifications Validity - All work products must satisfy the requirements of the Government as specified herein.

File Editing - All text and diagrammatic files shall be editable by the Government.

Timeliness - Work products shall be submitted on or before the due date specified in this Task Order.

Format – Microsoft Office 2003 file format.

9.0 Government Furnished Equipment and Materials

9.1 Government Furnished Equipment

For each person covered under this contract, the Office of Information and Technology shall provide:

- A standard-sized working area (cube)
- A personal computer (PC) with CBP standard desktop applications
- Standard PC input devices and perphrials, i.e., a mouse, a keyboard, a monitor
- A connection to the OIT Local Area Network (LAN)
- A connection to an OIT LAN printer.

9.2 Government Furnished Materials

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 required information and materials and provide the request at least 30 days in advance of requested delivery.

10.0 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.

11.0 Section 508 Requirements

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

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

11.1 36 CFR 1194.21 – Software Applications and Operating Systems

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.

11.2 36 CFR 1194.22 –Web-Based and Internet Information Applications

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.

11.3 36 CFR 1194.31 – Functional Performance Criteria

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.

11.4 36 CFR 1194.41 – Information Documentation and Support

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 shall be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

11.5 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.

11.6 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 shall 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.

12.0 Enterprise Architecture Requirements

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

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

(c) 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.

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

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

13.0 Security Requirements

All services provided under this task order must be compliant with DHS Information Security Policy, identified in MS4300.1, *Information Technology Systems Security Program* and *4300A Sensitive Systems Handbook.*

13.1 Security Requirements for Unclassified Information Technology Resources

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

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

(1) Within 60 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

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

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation shall proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer shall provide upon request. This accreditation shall 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.

13.2 Contractor Employee Access

(a) *Sensitive Information,* as used in this Section, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to

which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

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

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

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

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

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

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

13.3 Security Certification/Accreditation

CBP shall provide personnel with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with DHS MD 4300A, DHS Sensitive Systems Policy and Handbook. During all SDLC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation shall be performed using the DHS certification/accreditation process, methodology and tools.

13.4 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 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.

13.5 Security Procedures

13.5.1 Controls

The Contractor shall comply with the Bureau of Customs and Border Protection (CBP) administrative, physical and technical security controls to ensure that the Government's security requirements are met.
Identification Badges

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

13.5.2 Security Background Data

A Contractor employee shall not begin working under the contract until the entire background investigation (BI) is completed with approval from CBP, Security Programs Division. Exceptions to this requirement shall be handled on a case-by-case basis, and access to facilities, systems, data, etc. shall be limited until the individual is cleared.

Contractor employee personnel hired to work within the United States or its territories and possessions that require access to CBP facilities, information systems, security items and products, and/or sensitive but unclassified information shall either be U.S. citizens or have lawful permanent resident status.

The following security screening requirements apply to both U.S. citizens and lawful permanent residents who are hired as Contractor personnel. All personnel employed by the Contractor or responsible to the Contractor for the performance of work hereunder shall either currently possess or be able to favorably pass a background investigation. The Contractor shall submit within ten (10) working days after award of this contract a list containing the full name, social security number, and date of birth of these people who claim to have successfully passed a background investigation by the CBP, or submit such information and documentation as may be required by the Government to have a BI performed for all personnel. The information must be correct and be reviewed by a Customs Official for completeness. Normally this shall consist of SF-85P, "Questionnaire for Public Trust Positions;" FD-258, "Fingerprint Chart;" and a Financial Statement.

Failure of any Contractor personnel to pass a BI means that the Contractor has failed to satisfy the contract's requirement to provide cleared personnel. The continuing failure to meet the requirement to provide cleared personnel is grounds for termination of the contract, unless cleared personnel are timely provided as replacements. The Contractor must provide a qualified replacement capable of passing a BI for any person who fails to successfully pass a BI. This policy also applies to any personnel hired as replacements during the term of the contract. The Contracting Officer must approve all personnel replacements.

Estimated completion of the investigation is approximately ninety (90) to one hundred twenty (120) days from the date the completed forms are received in the Security Programs Division.

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."*

13.5.3 Notification of Personnel Changes

The Contractor shall notify the Contracting Officer's Technical Representative and Contracting Officer via phone, FAX, or electronic transmission, no later than one workday after any personnel changes occur. Written confirmation is required for phone notification. This includes, but is not limited to, name changes, resignations, terminations, and reassignments (i.e., to another contract.)

The Contractor shall notify the OIT Information Systems Security Branch (ISSB) of any change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other Contractors. The Contractor shall provide the following information to OIT ISSB at TEL: (703) 921-6116 and FAX (703) 921-6570: full name, social security number, effective date, and reason for change.

13.5.4 Separation Procedure

In accordance with Customs Directive No. 51715-006, "Separation Procedures for Contractor Employees," the Contractor is responsible for ensuring that all separating employees complete relevant portions of the Contractor Employee Separation Clearance, Customs Form 242. This requirement covers all Contractor employees who depart while a contract is still active (including resignation, termination, etc.) or upon final contract completion. Failure of a Contractor to properly comply with these requirements shall be documented and considered when completing Contractor Performance Reports.

13.5.5 General Security Responsibilities During Performance

The Contractor shall ensure that its employees follow the general procedures governing physical, environmental, and information security described in the various CBP regulations pertaining thereto, good business practices, and the specifications, directives, and manuals for conducting work to generate the products as required by this contract. Personnel shall be responsible for the physical security of their area and government furnished equipment (GFE) issued to them under the provisions of the contract.

13.5.6 Non-Disclosure Agreements

Upon award, the contractor shall provide to the COTR a signed DHS 11000-6 Standard Non-Disclosure Agreement Form for each employee working under the contract. The contractor shall also provide this signed form each time a new employee is assigned to the contract.

13.5.7 Information Security

"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.*

14.0 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]

15.0 Period of Performance

The period of performance for this task statement includes a one-year (12 month) base period and four option periods of 12 months each. The option periods, should they be exercised, are found in Table 5.

Table 5. Base and Option Periods of Performance

Period	Term
Base Period	12 months
Option Period 1	12 months
Option Period 2	12 months
Option Period 3	12 months
Option Period 4	12 months

16.0 Place of Performance

16.1 Location

Contractors shall identify those services that must be performed onsite and shall provide the number and type of workstations needed for onsite services. CBP shall provide office space at OIT program offices and Enterprise Test labs located within a 50-mile radius of Washington, DC for services that must be conducted onsite. CBP office space in the Washington, DC area is limited and Contractors are encouraged to propose alternative solutions as appropriate to the services required in this SOW.

Services ordered under this Task Order for ELCM/PAL support shall be performed at the National Data Center (NDC) located in Springfield, Virginia. Performance may also be required at current or future U.S. Customs locations in the Washington, DC Metropolitan area.

Task Order personnel may be required to work full-time, part-time or attend meetings at any location within the 50-mile radius of the Washington, DC Metropolitan area.

Currently, the CBP sites where it is anticipated that the majority of the work shall be performed are as follows:

US Customs and Border Protection
7501 Boston Boulevard, NDC-2
Springfield, VA 22153

16.2 Other Locations Where Work May be Required

US Customs and Border Protection
7681 Boston Boulevard, NDC-1
Springfield, VA 22153

US Customs and Border Protection
7400 Fullerton Road, NDC-3
Springfield, VA 22153

US Customs and Border Protection
7451 Boston Boulevard, NDC-4
Springfield, VA 22153

US Customs and Border Protection
7435 Boston Boulevard, NDC-5
Springfield, VA 22153

US Customs and Border Protection
2850 Eisenhower Avenue
Alexandria, VA 22314

US Customs and Border Protection
1801 N. Beauregard Boulevard
Alexandria, VA 22311

US Customs and Border Protection
7375 Boston Boulevard, Boston's
Springfield, VA 22153

US Customs and Border Protection
7971 Kingstown Village Parkway, Suite 500
Springfield, VA 22315

US Customs and Border Protection
Headquarters
1300 Pennsylvania Ave., NW
Washington, DC 20229

US Customs and Border Protection
1331 Pennsylvania Ave., NW, (National Place)
Washington, DC 20229

16.3 Telecommuting

The Contractor and the Government must agree on the terms and conditions.

17.0 Travel and Other Direct Costs

The Government anticipates the requirement of other direct costs and occasional other than local travel within the metropolitan area.

Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility (i.e., designated work site) shall not be reimbursed hereunder. For other than local travel, written approval is required from the COTR or Contracting Officer. Costs associated with Contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs.

18.0 Billing and Invoices

18.1 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
- Copies of signed time sheets/cards covering the hours claimed on the invoice
- 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

18.2 Invoicing Submission and Deadlines

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

Invoices for hours worked in a given month shall be submitted to the National Finance Center and the COTR 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 COTR no later than the 20th day of June 2009.

19.0 Government Contacts

19.1 Executive Leads

19.1.1 Primary Executive Lead

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

19.1.2 Alternate Executive Lead

Name: (b) (6)
Telephone Number: (703 (b) (6)

Email: (b) (6) @dhs.gov

19.2 Contracting Officer's Technical Representative (COTR):

19.2.1 Primary COTR

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

19.2.2 Alternate Technical Point of Contact

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

Appdenix A Acronyms

Acronym	Meaning
BI	Background Investigation
CBP	U.S. Customs and Border Protection
CBT	Computer Based Training
CFR	Code of Federal Regulations
CM	Configuration Management
COTR	Contracting Officer's Technical Representative
COTS	Commercial-Off-the-Shelf (software)
DC	District of Columbia
DDC	OIT Deputy Director's Council
DHS	Department of Homeland Security
EA	Enterprise Architecture
EDME	Enterprise Data Management and Engineering Division.
EDMO	DHS Enterprise Data Management Office
EIT	Electronic Information Technology
ELCM	Enterprise Life Cycle Methodology
EVM	Earned Value Management
EV&TS	ELCM Vision and Transition Strategy
FAR	Federal Acquisition Regulations
FOC	Final Operating Capability
FTE	Full Time Equivalent
GFE	Government-Furnished Equipment
GOTS	Government-Off-the-Shelf (software)
HLS	Homeland Security
ISSB	OIT Information Systems Security Branch
IT	Information Technology
IOC	Initial Operating Capability
MD	Management Directive
OAST	DHS Office on Accessible Systems and Technology
OIT	Office of Information and Technology
OMB	Office of Management and the Budget
PAL	Process Asset Library
PCII	Protected Critical Infrastructure Information
P.L.	Public Law
PMB	Process Management Branch
PTR(s)	Problem Trouble Reports
SLC	Systems Life Cycle
SOW	Statement of Work
SSI	Sensitive Security Information
TO	Task Order
U.S.C.	US Code
WBS	Work Breakdown Structure