

EPIC v. CBP, No. 14-cv-01217-RBW
Plaintiff's Combined Opposition to Defendant's Motion for Summary Judgment and
Cross-Motion for Summary Judgment

Exhibit 2

AFI

Analytical Framework for Intelligence

The Office of Intelligence and Investigative Liaison (OIIL) has embarked on the development of U.S. Customs and Border Protection's (CBP) (b) (7)(E)

The Analytical Framework for Intelligence (AFI) will (b) (7)(E)

(b) (7)(E)

It further (b) (7)(E)

As a system, (b) (7)(E)

For more information on AFI, please contact:

(b) (7)(C), (b) (6)



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

U.S. Customs and Border Protection
Office of Intelligence and Investigative Liaison
1300 Pennsylvania Avenue, NW
Washington, DC 20229

(b) (7)(C), (b) (6)

www.cbp.gov

August 2011

CBP_OI L - (b) (7)(C), (b) (6)
000001



AFI

Analytical Framework for Intelligence



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

GOALS AND CAPABILITIES

AFI's goal is to (b) (7)(E)



AFI is a

(b) (7)(E)

• (b) (7)(E)

KEY FEATURES

1. Improved Effectiveness and Efficiency
2. Improved (b) (7)(E)
3. Greater (b) (7)(E)
4. Improved (b) (7)(E)
5. Improved Capabilities
6. Adherence to All Privacy and Security Policies

BUILDING ON CURRENT SYSTEM CAPABILITIES

• (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

• Access to many (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)



U.S. DEPARTMENT OF HOMELAND SECURITY

U.S. Customs and Border Protection • Office of Intelligence and Investigative Liaison

OIII

“Value-Added Intelligence Supporting America’s Frontline”



Analytical Framework for Intelligence

(U) Warning: This document contains UNCLASSIFIED // FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official.

(U) Requests for use or further dissemination of any material contained herein should be made to: Assistant Commissioner, CBP Office of Intelligence and Investigative Liaison, 1300 Pennsylvania Avenue, NW, Washington, DC 20229, by phone at (b) (6), (b) (7)(C) or by email at (b) (7)(C), (b) (6).

000003



What is AFI?

- AFI is a multi-year investment to provide collection, production and dissemination of intelligence information.

- AFI is a multi-year investment to provide collection, production and dissemination of intelligence information. (b) (7)(E)

(b) (7)(E)

- The AFI program provides a full suite of tools designed to enhance analysts' all-source intelligence capability within:

- Data Consolidation & Research
- Analysis
- Collaboration & Reporting
- Production Management

(b) (7)(E)





Current State & Future Goals

- Legacy systems are not sufficiently integrated

- (b) (7)(E)

- Address and leverage the strengths of existing functional and analytical capabilities

- Increase efficiency and effectiveness of CBP intelligence analysts
 - Facilitate and consolidate access to existing CBP data sources
 - Integrate analytical tools and methods
 - Enhance collaboration and information sharing between analysts
 - Augment reporting and metrics





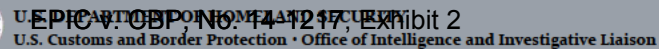
System Integration

- **AFI funds and enhances current systems:**

(b) (7)(E)

(b) (7)(E)

(b) (7)(E)



000006

~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

Plaintiff's Cross-Motion for Summary Judgment



Current State

- **AFI – Operational as of 8/10/2012**

- Over (b) (7)(E) users at more than (b) (7)(E) locations spread between 8 CBP

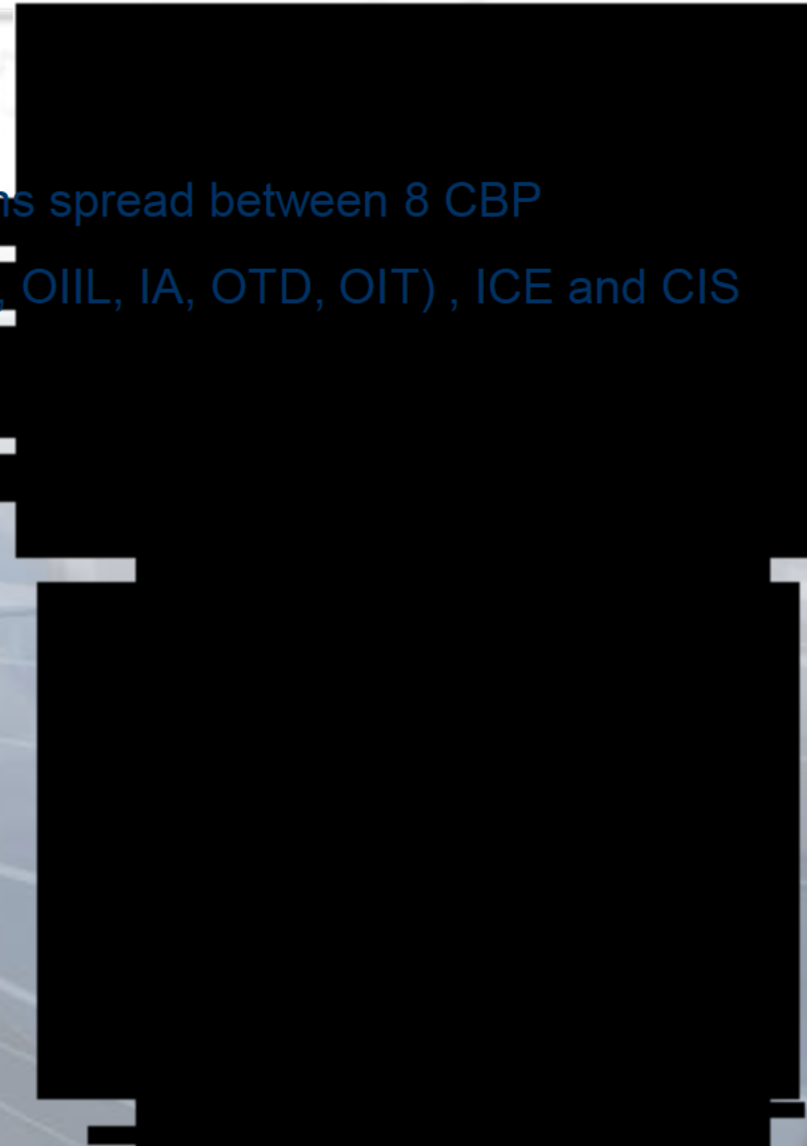
- organizational units (OBP, OFO, OT, OAM, OIIL, IA, OTD, OIT) , ICE and CIS

- **Network Deployment – (b) (7)(E)**

- (b) (7)(E) Facilities across the U.S.

- (b) (7)(E) Secure Video Conference

- (b) (7)(E) within CBP





~~UNCLASSIFIED // FOR OFFICIAL USE ONLY~~

Analytical Framework for Intelligence Operational Status & Security

Operational Status

The Analytical Framework for Intelligence (AFI) is an integrated intelligence system being developed to support CBP's evolution as (b) (7)(E) organization. On August 12, 2012, AFI went live and became an official operating system.

Key capability areas that AFI currently provides, or will provide in the future, include: Data Consolidation and Research, Analysis, Production Management, Collaboration, and Reporting. Please see the attached tri-fold for more information. AFI will deliver (b) (7)(E) to CBP over the next (b) (7)(E) with new releases every (b) (7)(E).

For additional information on AFI please refer to the following documents:

[AFI Privacy Impact Assessment](#)¹

[AFI System of Records Notice](#)²

[AFI System of Records Notice – Notice of Proposed Rulemaking](#)³

[AFI System of Records Notice – Final Rule](#)⁴

Security Basics

AFI and Palantir are authorized to store/process sensitive but unclassified data and information (SBU). AFI and Palantir cannot (b) (7)(E)

The AFI and Palantir data/information is stored on (b) (7)(E)

The CBP AFI and Palantir data are accessible to AFI users with the (b) (7)(E) in their user profile. Access to AFI (b) (7)(E)

Access to AFI (b) (7)(E)

¹ http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_afi_june_2012.pdf

² <http://www.gpo.gov/fdsys/pkg/FR-2012-06-07/html/2012-13813.htm>

³ <https://www.federalregister.gov/articles/2012/06/07/2012-13815/privacy-act-of-1974-implementation-of-exemptions-department-of-homeland-security-us-customs-and>

⁴ <https://www.federalregister.gov/articles/2012/08/10/2012-19336/privacy-act-of-1974-implementation-of-exemptions-department-of-homeland-security-us-customs-and>

The data from AFI and Palantir can be shared with other stakeholder and agencies if a memorandum of understanding or task force agreement is in place or in accordance with routine uses as documented in the AFI System of Records Notice. As always, use the third party rule when sharing information. Please refer to the AFI Privacy Impact Assessment and System of Record Notice for more information and detail – these documents outline in detail what information can be shared and with whom.

Please direct questions on any AFI operational or security issue to (b) (7)(E)

SUMMARY OF AFI ROLES FOR RELEASE 6.0

AFI ROLE	CAPABILITIES	Usage
(b) (7)(E)	Browse/Search (b) (7)(E) (b) (7)(E) Perform (b) (7)(E) (b) (7)(E) View/Manage Preferences (b) (7)(E)	Browsing and Searching (b) (7)(E) (b) (7)(E)
(b) (7)(E)	(b) (7)(E) (b) (7)(E) (b) (7)(E) Export (b) (7)(E) where applicable View and respond (b) (7) Review submitted (b) (7)(E) View/Manage (b) (7) View/Manage (b) (7) View/Manage (b) (7)(E)	(b) (7)(E) (b) (7)(E) (b) (7)(E)
(b) (7)	(b) (7)(E) Export (b) (7)(E) (b) (7)(E)	(b) (7)(E) (b) (7)(E)
(b) (7)(E)	(b) (7)(E) Create/Edit/Save/Submit (b) (7)(E) Review (b) (7)(E) View/Manage (b) (7)(E)	Allows users to (b) (7) (b) (7)(E) (b) (7)(E) (b) (7)(E)
(b) (7)(E)	(b) (7)(E) Create/Edit/Save/Submit (b) (7)(E) (b) (7)(E) View/Manage (b) (7)(E)	Allows users to (b) (7) (b) (7)(E) (b) (7)(E)
(b) (7)(E)	(b) (7)(E) Create/Edit/Save/Submit (b) (7) View/Manage (b) (7)(E)	Allows users to (b) (7)(E) (b) (7)(E)
(b) (7)(E)	(b) (7)(E) (b) (7)(E) View/Manage (b) (7)(E)	Allows users to (b) (7)(E) (b) (7)(E) (b) (7)(E)
(b) (7)(E)	(b) (7)(E) (b) (7)(E)	Currently covered by (b) (7) (b) (7)(E) Allows (b) (7)(E) users to (b) (7)(E) (b) (7)(E) (b) (7)(E)

AFI ROLE	CAPABILITIES	Usage
(b) (7)(E)	(b) (7)(E) Edit (b) (7)(E) Create/Edit/Save/Submit (b) (7)(E) Edit (b) (7)(E) Publish (b) (7)(E) (b) (7)(E)	This role is (b) (7)(E); allows users to (b) (7)(E). Also allows users to (b) (7)(E)
(b) (7)(E)	(b) (7)(E)	This is a (b) (7)(E)
(b) (7)(E)	(b) (7)(E) Approve/Reject (b) (7)(E) View/Manage (b) (7)(E)	This role is (b) (7)(E); allows users to (b) (7)(E)
(b) (7)(E)	(b) (7)(E) (b) (7)(E) View/Manage (b) (7)(E)	This is a (b) (7)(E); allows users to (b) (7)(E)
(b) (7)(E)	RESTRICTED	RESTRICTED

(b) (7)(E); do not select

(b) (7)(E)

Transition to New Roles in AFI 6.0

Existing User Has the Current Role:	Existing User Assigned these Roles in 6.0 Automatically:
(b) (7)(E)	(b) (7)(E)
(b) (7)	(b) (7)(E)

AFI User Security Access Definitions

The following definitions assist users in determining which options to select in the (b) (7)(E) of the AFI (b) (7)(E). (b) (7)(E) impacts the (b) (7) a user will be able to (b) (7)(E).

- AFI Users: Select the (b) (7)(E) for the (b) (7)(E) that you have (b) (7)(E).
- AFI Supervisors: Approve the (b) (7)(E) for the (b) (7)(E) that (b) (7)(E).

For Official Use Only (FOUO): The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, 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 interest. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958, "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Products that are identified as FOUO upon uploading into AFI (b) (7)(E) will have the (b) (7)(E). Only users that have a need to know for FOUO information in the normal performance of their daily duties will have access to information identified as FOUO.

Protected Critical Infrastructure Information (PCII): Critical infrastructure information (as defined in 6 U.S.C. 131(3)), means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.

Products that are identified as PCII upon uploading into AFI (b) (7)(E) will have the (b) (7)(E). Only users that have a need to know for PCII information in the normal performance of their daily duties will have access to information identified as PCII.

Sensitive Security Information (SSI): Sensitive security information (SSI), as defined in 49 C.F.R. Part 1520, is a specific category of information that requires protection against disclosure. 49 U.S.C. 40119 limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.

Products that are identified as SSI upon uploading into AFI (b) (7)(E) will have the (b) (7)(E). Only users that have a need to know for SSI information in the normal performance of their daily duties will have access to information identified as SSI.

Law Enforcement Sensitive (LES): The designation used to protect information compiled for law enforcement purposes. LES is a subset of FOUO.

Products that are identified as LES upon uploading into AFI (b) (7)(E) will have the (b) (7)(E). Only users that have a need to know for LES information in the normal performance of their daily duties will have access to information identified as LES.

Passenger Name Record (PNR): A record in the database of a Computer Reservation System (CRS) that contains the itinerary for a passenger or a group of passengers traveling together. A PNR typically contains more information of a sensitive nature, including the passenger's full name, date of birth, home and work address, telephone number, e-mail address, credit card details, IP address if booked online, as well as the names and personal information of emergency contacts.

Products that are identified as PNR upon uploading into AFI (b) (7)(E) will have the (b) (7)(E). Only users that have a need to know for PNR information in the normal performance of their daily duties will have access to information identified as PNR.

Bank Secrecy: The United States' Bank Secrecy Act (or BSA) requires financial institutions to assist government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding \$10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.

Products that are identified as Bank Secrecy upon uploading into AFI (b) (7)(E) will have the (b) (7)(E). Only users that have a need to know for Bank Secrecy information in the normal performance of their daily duties will have access to information identified as Bank Secrecy.

Trade Sensitive Information: The designation is used for information pertaining to U.S. Trade Policy, strategies and negotiating objectives.

Products that are identified as Trade Sensitive upon uploading into AFI (b) (7)(E) will have the (b) (7)(E). Only users that have a need to know for Trade Sensitive information in the normal performance of their daily duties will have access to information identified as Trade Sensitive.

US Persons: This designation is used to identify products or information that would need additional review prior to release to elements of the Intelligence Community, due to the inclusion of specific identifying characteristics of United States persons in the product or information.

50 USC and Executive Order 12333 define US Persons as:

- a citizen of the United States,

- an alien lawfully admitted for permanent residence,
- an unincorporated association with a substantial number of members who are citizens of the U.S. or are aliens lawfully admitted for permanent residence, or
- a corporation that is incorporated in the U.S. except for a corporation directed and controlled by a foreign government or governments.

Products that are identified as US Persons upon uploading into AFI (b) (7)(E) will have the (b) (7)(E). Only users that have a need to know for US Persons information in the normal performance of their daily duties will have access to information identified as US Persons.

**Department of Homeland Security
Customs & Border Protection (CBP)
Targeting and Analysis Systems Program Directorate**

Statement of Work (SOW)

1.0 OVERVIEW AND BACKGROUND

The mission of The Department of Homeland Security (DHS) is to lead the unified national effort to secure America. DHS prevents and deters terrorist attacks and protects against and responds to threats and hazards to the nation. DHS ensures safe and secure borders, welcomes lawful immigrants and visitors, and promotes the free-flow of commerce.

The purpose of the Analytical Framework for Intelligence (AFI) is to define, design and implement an information framework to support the ever growing and expanding needs of analysis of intelligence data across various network domains. AFI is a suite of analytical software applications and infrastructure tools integrated into a single powerful platform that allows intelligence analysts to visualize and analyze large amount of data from disparate data sources utilizing existing and future hardware and software.

2.0 OBJECTIVES

In support of the AFI project, Customs and Border Protection (CBP) has a need to access commercially available subscription based data as XML data feeds. These XML data feeds are designed to support the screening, targeting, and tracking of persons that are currently or have been in the United States or are tied to entities within the United States.

3.0 SCOPE OF WORK

CBP expects the vendor to deliver the data feeds described in Section 4.0 in an XML format when requested by the AFI application for the period of performance.

4.0 DELIVERABLES

Item No.	Description
001	(b) (7)(E) up to 13,000 per month- Period of Performance 1/1/2015 to 12/31/2015 –XML Feed
002	(b) (7)(E) – 4,000 per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
003	(b) (7)(E) – 13,000 per month - Period of Performance 1/1/2015 to

	12/31/2015–XML Feed
004	(b) (7)(E) - 1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
005	(b) (7)(E) - 1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
006	(b) (7)(E) - 1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
007	(b) (7)(E) -1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
008	(b) (7)(E) -1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed
009	(b) (7)(E) -1000 hits per month - Period of Performance 1/1/2015 to 12/31/2015–XML Feed

5.0 PERIOD OF PERFORMANCE AND LOCATION

Period of Performance: January 1, 2015 to December 31, 2015.

Location: Contractor facilities.

6.0 INVOICING AND PAYMENT

Invoices shall be electronically transmitted to the Point of Contact listed in section 7.0. To constitute a proper invoice, each invoice shall be annotated with at least the following information:

- Order number
- Description of services provided for a specified time period.
- Unit price and total amount of each item.
- Discount terms
- Company name, telephone number, taxpayer's identification number, and complete mailing address to which payment will be mailed.

Copies of invoices (paper submissions) will be submitted to the following addresses *OR as an alternative*, to the email addresses cited below:

1. **Payment Center:**

DHS/U.S. Customs and Border Protection
National Finance Center/Commercial Accounts
P. O. Box 68908
Indianapolis, Indiana 46268

OR as an alternative:

Email: cbpinvoices@dhs.gov

2. Contracting Officer's Representative

DHS/U.S. Customs and Border Protection
Attention: (b) (6)
5971 Kingstowne Village Pkwy
5th Floor Mailroom
Alexandria, VA 22315

Email: (b) (6)

3. Contracting Officer's Representative - Alternate

DHS/U.S. Customs and Border Protection
Attention: (b) (6)
5971 Kingstowne Village Pkwy
5th Floor Mailroom
Alexandria, VA 22315

Email: (b) (6)

3. TASP Budget POC

DHS/U.S. Customs and Border Protection
Attention: (b) (6)
5971 Kingstowne Village Pkwy
5th Floor Mailroom
Alexandria, VA 22315

Email: (b) (6)

Only the contracting officer has the authority to represent the Government in cases where the task order requires a change in the terms and conditions, delivery schedule, scope of work and/or price of the products and/or services under this task order.

7.0 POINT OF CONTACT

CONTRACTING OFFICER'S REPRESENTATIVE

(b) (6)

Customs & Border Protection
Office of Information & Technology
Targeting and Analysis Systems Program Directorate
5971 Kingstowne Village Parkway
Fifth Floor Mailroom
Alexandria, VA 22315
Office phone: (b) (6)
E-mail: (b) (6)

CONTRACTING OFFICER'S REPRESENTATIVE – ALTERNATE

(b) (6)

Customs & Border Protection
Office of Information & Technology
Targeting and Analysis Systems Program Directorate
5971 Kingstowne Village Parkway
Fifth Floor Mailroom
Alexandria, VA 22315
Office phone: (b) (6)
E-mail: (b) (6)

8.0 Clauses

The Contractor shall fulfill the duties of this SOW while maintaining full compliance with all terms and conditions of the contract. Please see below for IT security and agency specific clauses applicable to this contract.

Enterprise Architecture (EA) Compliance

The Offeror shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the [DHS Service Oriented Architecture - Technical Framework](#)), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA).

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. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be

in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

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

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

All IT hardware and software shall be compliant with the HLS EA.

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

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

Compliance with DHS Security Policy Terms and Conditions

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

Encryption Compliance

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

(b) (7)(E)

(b) (7)(E)

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

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

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

(1) Within 15 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 information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer.

Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 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.

CONTRACTOR EMPLOYEE ACCESS (JUN 2012)

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

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

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

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

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

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

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

background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

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

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

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

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

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

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

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

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

- (1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
- (2) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

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

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

Required Protections for DHS Systems Hosted in Non-DHS Data Centers

Security Authorization

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.

At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture to the best of its ability and to the satisfaction of the DHS COR. Areas of consideration could include:

(b) (7)(E)



5) Performance of activities per continuous monitoring requirements

Continuous Monitoring

The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

1. Asset Management
2. Vulnerability Management
3. Configuration Management
4. Malware Management
5. Log Integration
6. Security Information Event Management (SIEM) Integration
7. Patch Management
8. Providing near-real-time security status information to the DHS SOC

Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

Security Operations

The Contractor shall operate a SOC to provide the security services described below. The Contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. The contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility SOC shall adhere to the incident response plan.

Computer Incident Response Services

The Contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident

Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

Firewall Management and Monitoring

The Contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Intrusion Detection Systems and Monitoring

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. (b) (7)(E)

The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Physical and Information Security and Monitoring

The Contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

Vulnerability Assessments

The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

Anti-malware (e.g., virus, spam)

The Contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly

status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Patch Management

The Contractor shall perform provide patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. All other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained (b) (7)(E).

Personal Identification Verification (PIV) Credential Compliance

Authorities:

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 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.

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.

OAST (Office on Accessible Systems and Technology) Compliance

Accessibility Requirements (Section 508)

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

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

Section 508 Applicable EIT Accessibility Standards

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

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

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

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

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the 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.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

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

ISO (Information Security) COMPLIANCE

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*.

Interconnection Security Agreements

Interconnections between DHS and non-DHS IT systems shall be established only 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.

System Security documentation appropriate for the SELC status.

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.

Disaster Recovery Planning & Testing – Hardware

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.

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 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.

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 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.

Monitoring/reviewing contractor security requirements clause

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 Technical 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.

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

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


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.

Engineering Platforms

Common Enterprise Services (CES) – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. (b) (7)(E)



(b) (7)(E)



ITP (Infrastructure Transformation Program) COMPLIANCE

Help Desk and Operations Support

The contractor shall provide third tier reporting for trouble calls received from the Help Desk, the DHS Task Manager, or the users. The Contractor shall respond to the initiators of trouble calls as by receiving telephonic notifications of problems, resolving them, or directing them to the proper technical personnel for resolution. Problems that cannot be resolved immediately or with the requirements of the performance standards are to be brought to the attention of the DHS Task Manager. The Contractor shall document notification and resolution of problems in Remedy.

Interfacing

As requested by the COR, assistance in consolidating all systems with the DHS Consolidated Data Center. Resources to be consolidated with the DHS Consolidated Data Center for each system to be determined by the COR.

TRANSITION PLAN

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

- Coordination with Government representatives

- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

Portfolio Review

Screening/Watchlist/Credentialing

Includes all activities that support the tracking and monitoring of travelers, conveyances and cargo crossing U.S. borders, and traffic pattern analysis, database (Federal, State, and Local) linking and querying, and managing status verification and tracking systems. Different investments and systems may support distinct screening and watchlist activities for people, cargo, and tangible goods. Credentialing encompasses all activities that determine a person's eligibility for a particular license, privilege, or status, from application for the credential through issuance, use, and potential revocation of the issued credential.

**Department of Homeland Security
Customs & Border Protection (CBP)
Targeting and Analysis Systems Program Office**

Statement of Work (SOW)

1.0 OVERVIEW AND BACKGROUND

The mission of The Department of Homeland Security (DHS) is to lead the unified national effort to secure America. DHS prevents and deters terrorist attacks and protects against and responds to threats and hazards to the nation. DHS ensures safe and secure borders, welcomes lawful immigrants and visitors, and promotes the free-flow of commerce.

The purpose of the Analytical Framework for Intelligence (AFI) is to define, design, and implement an information framework to support the ever growing and expanding needs of analysis of intelligence data across various network domains. AFI will be a suite of analytical software applications and infrastructure tools integrated into a single powerful platform that will allow intelligence analysts to visualize and analyze large amount of data from disparate data sources utilizing existing and future hardware and software. AFI will host or provide easy access to classified and non-classified data currently located on various systems from different sources and government agencies, and will provide the backbone to achieve the goal of minimizing time spent on data collection and maximize the time spent on analysis.

The planned functionality of AFI will be to integrate "best in breed" GOTS/COTS applications and reuse existing software components to:

- Provide a data consolidation and research platform
- Provide an analysis platform
- Provide a production management platform
- Provide a collaboration and reporting platform

2.0 OBJECTIVES

In support of the AFI project, Customs and Border Protection (CBP) will implement solutions to enable CBP to begin to significantly upgrade data management capabilities by obtaining commercially available subscription based data as an XML data feeds. These XML data feeds are feed designed to support the screening, targeting, and tracking of persons that are currently or have been in the United States or are tied to entities within the United States.

3.0 SCOPE OF WORK

CBP expects the vendor to deliver the data feeds described in Section 4.0 in an XML format when requested by the AFI application:

4.0 DELIVERABLES

Item No.	Description
001	Landline Data (LexisNexis) - (b) (7)(E) up to 13,000- Period of Performance 1/1/2013 to 12/31/2013 –XML Feed
002	(b) (7)(E) - 4,000 per month - Period of Performance 1/1/2013 to 12/31/2013–XML Feed
003	(b) (7)(E) - 13,000 per month - Period of Performance 1/1/2013 to 12/31/2013–XML Feed
004	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013–XML Feed
005	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013–XML Feed
006	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013–XML Feed
007	(b) (7)(E) 000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013–XML Feed
008	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013–XML Feed
009	(b) (7)(E) 1000 hits/mo - Period of Performance 1/1/2013 to 12/31/2013–XML Feed

PERIOD OF PERFORMANCE, LOCATION AND HOURS OF PERFORMANCE

Period of Performance: 1/1/2013-12/31/2013

Location:

US Customs & Border Protection
Targeting and Analysis Systems Program Office
5971 Kingstowne Village Parkway
Fifth Floor Mailroom
Alexandria, VA 22315

And contractor facilities.

4.0 INVOICING AND PAYMENT

The contractor shall submit one invoice for the hardware cost. Invoices shall be electronically transmitted to the Technical Point of Contact listed in section 5.0. To constitute a proper invoice, each invoice shall be annotated with at least the following information:

- Order number
- Description of services provided for a specified time period.
- Unit price and total amount of each item.
- Discount terms
- Company name, telephone number, taxpayer's identification number, and complete mailing address to which payment will be mailed.

Only the contracting officer has the authority to represent the Government in cases where the task order requires a change in the terms and conditions, delivery schedule, scope of work and/or price of the products and/or services under this task order.

5.0 POINT OF CONTACT

CONTRACTING OFFICER'S REPRESENTATIVE

(b) (6)

Customs & Border Protection
Office of Information & Technology
Targeting and Analysis Systems Program Office
5971 Kingstowne Village Parkway
Fifth Floor Mailroom
Alexandria, VA 22315

Office phone: (b) (6)

e-mail: (b) (6)

6.0 DHS Clauses

Enterprise Architecture (EA) Compliance

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

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model as described in their respective EAs. Models will be submitted using Business Process Modeling Notation (BPMN) version 2.0 and the CBP Architectural Modeling Standards for all models. Universal Modeling Language (UML2) may be used for infrastructure only. Data exchange formats and semantics shall be in conformance with the

National Information Exchange Model (NIEM), version 2.0. Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

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

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

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

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

In compliance with Office of Management and Budget (OMB) mandates, all network hardware provided under the scope of this Statement of Work and

associated Task Orders (TO) shall be IPv6 compatible without modification, upgrade, or replacement.

OAST (Office on Accessible Systems and Technology) Compliance

- **DHS Accessibility Requirements Tool (DART)**

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

Accessibility Requirements (Section 508)

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

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

Section 508 Applicable EIT Accessibility Standards

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

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

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

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

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

Section 508 Applicable Exceptions

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

Section 508 Compliance Requirements

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

an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

EBMO (Investment Review) Compliance

- Legitimate Investments must be identified (on line 15 of the DHS Checklist) - based on Exhibit 53 (attached). Also, if more than 1 investment is identified – please split out the cost associated with each investment.

ISO (Information Security) COMPLIANCE

- **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*."

- **Interconnection Security Agreements**

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

- **HSAR Clauses**

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

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the

Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

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

(1) Within 15 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

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

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

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

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

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

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the

contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

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

HSAR 3052.204-71 Contractor Employee Access Clause

CONTRACTOR EMPLOYEE ACCESS (JUN 2006)

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

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

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

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

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

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

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

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

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

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

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

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

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

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

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO)

and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

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

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

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

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

- **System Security documentation appropriate for the SELC status.**

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.

Disaster Recovery Planning & Testing – Hardware (if applicable)

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.

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 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.

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 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.

- **Monitoring/reviewing contractor security requirements clause**

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 Technical Representative (COTR), 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.

- **Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information**

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

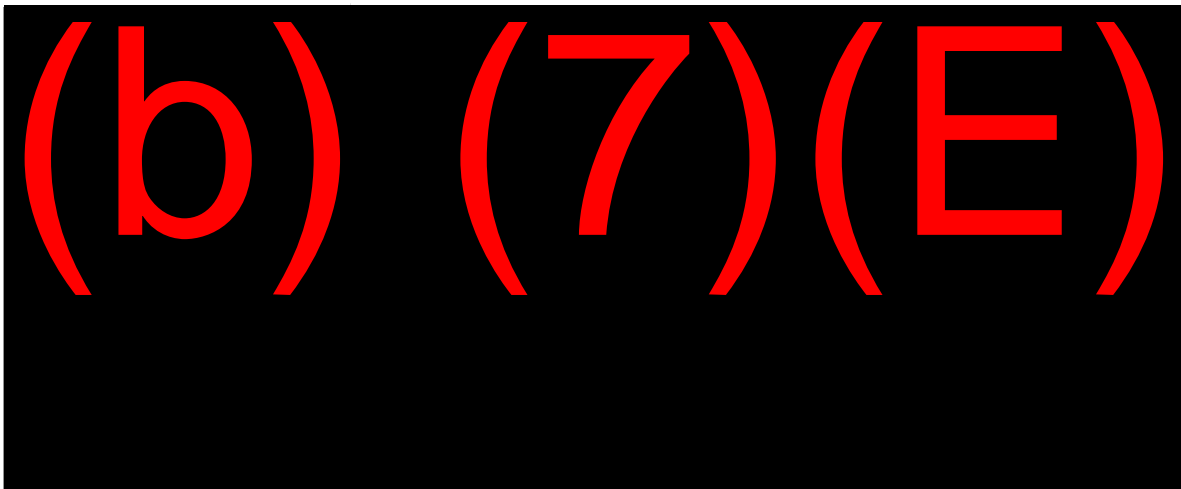
OMB-M-07-18 FDCC

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.

Engineering Platforms

- **Common Enterprise Services (CES)** – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. This

(b) (7)(E)



**ITP (Infrastructure Transformation Program) COMPLIANCE
(if applicable)**

- **Help Desk and Operations Support**

The contractor shall provide third tier reporting for trouble calls received from the Help Desk, the DHS Task Manager, or the users. The Contractor shall respond to the initiators of trouble calls as by receiving telephonic notifications of problems, resolving them, or directing them to the proper technical personnel for resolution. Problems that cannot be resolved immediately or with the requirements of the performance standards are to be brought to the attention of the DHS Task Manager. The Contractor shall document notification and resolution of problems in Remedy.

- **Interfacing**

As requested by the COTR, assistance in consolidating all systems with the DHS Consolidated Data Center. Resources to be consolidated with the DHS Consolidated Data Center for each system to be determined by the COTR.

TRANSITION PLAN (if applicable)

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

- Coordination with Government representatives

- Review, evaluation and transition of current support services
- Transition of historic data to new contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures

Portfolio Review

Screening/Watchlist/Credentialing

Includes all activities that support the tracking and monitoring of travelers, conveyances and cargo crossing U.S. borders, and traffic pattern analysis, database (Federal, State, and Local) linking and querying, and managing status verification and tracking systems. Different investments and systems may support distinct screening and watchlist activities for people, cargo, and tangible goods. Credentialing encompasses all activities that determine a person's eligibility for a particular license, privilege, or status, from application for the credential through issuance, use, and potential revocation of the issued credential.