SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
CISOIT17001	1	50

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
HSHQDC-13-D-E2065		HSSCCG-17-J-00004	HSSCCG-17-R-00002	11/28/2016

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	Kiley Leahy	802-872-4513	

9. ISSUED BY — CODE: CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

10. THIS ACQUISITION IS ☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % FOR:

☒ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ EDWOSB
☐ 8(A)

NAICS: 518210
SIZE STANDARD: $30.0

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
☐ SEE SCHEDULE	Net 30	☐	☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO — CODE: HQOIT

Department of Homeland Security
US Citizenship & Immigration Svcs
Office of Information Technology
111 Massachusetts Ave, NW
Suite 5000
Washington DC 20529

16. ADMINISTERED BY — CODE: CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

17a. CONTRACTOR/ OFFEROR — CODE: 9338881410000 — FACILITY CODE:

GLOBAL INFOTEK INC
1920 ASSOCIATION DRIVE SUITE 200
RESTON VA 201911543

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY — CODE: WEBVIEW

See Invoicing Instructions

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

☐ 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 933888141+0000 Joint Engineering Teams Sustainment - Entity Analytics (JETS-EA) The period of performance for this task order is 48 months, as follows: Transition-In: 1 month Base Period: 11 months Option 1: 12 months Option 2: 12 months Option 3: 12 months *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA: See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*: $5,133,898.00

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.
☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☒ 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR: Karen Emami

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*: Charles E. Julian

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
KAREN EMAMI, President	3/22/17	CHARLES E. JULIAN	3-22-17

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Dates will be adjusted based on the issuance of the notice to proceed (NTP). No invoicing may occur until after the NTP has been issued. The ultimate completion date of this task order may not extend beyond 9/8/21, per the EAGLE II contract. Two items were erroneously omitted from the Notice of Intent (NOI) that will now be added to the task order award, in accordance with FAR 52.252-4 Alterations in Contract: Portions of this contract are altered as follows: a) Under Section B, Travel funds are now included for each option period (rather than for the base period only, as originally reflected in the NOI). b) Under Section C, Task Order Clauses, addition of FAR 52.237-3 - Continuity of Services (Jan 1991). Global InfoTek's proposal, submitted on 12/10/16, and its Final Proposal Revision Addendum, submitted on 1/30/17, are hereby incorporated into the task order. AAP Number: None DO/DPAS Rating: NONE Accounting Info: ITRFRSP RFS EP 20-05-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Continued ...				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	Transition-In in accordance with PWS Section 5	1	MO	[redacted].00	[redacted].00
0002	Agile Teams (FFP)	11	MO	[redacted].00	[redacted].00
0003	ODCs Travel - In accordance with PWS Section 7.4	1	LO	59,400.00	59,400.00
1002	FFP Agile Teams Amount: [redacted](Option Line Item) Anticipated Exercise Date:03/16/2018	12	MO	[redacted].00	0.00
1003	ODCs Travel - In accordance with PWS Section 7.4 Amount: $59,400.00(Option Line Item) Anticipated Exercise Date:03/16/2018	1	LO	59,400.00	0.00
2002	FFP Agile Teams Amount: [redacted](Option Line Item) Anticipated Exercise Date:03/16/2019	12	MO	[redacted].00	0.00
2003	ODCs Travel - In accordance with PWS Section 7.4 Amount: $59,400.00(Option Line Item) Anticipated Exercise Date:03/16/2019	1	LO	59,400.00	0.00
3002	FFP Agile Teams Amount: [redacted]Option Line Item) Anticipated Exercise Date:04/16/2020	12	MO	[redacted].00	0.00
3003	ODCs Travel - In accordance with PWS Section 7.4 Amount: $59,400.00(Option Line Item) Anticipated Exercise Date:03/16/2020	1	LO	59,400.00	0.00

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Task Order Points of Contact: Contracting Officer's Representative (COR) Emily Chu Email: Emily.H.Chu@uscis.dhs.gov Phone: (202)272-1622 Contract Specialist (CS) Kiley Leahy Email: Kiley.M.Leahy@uscis.dhs.gov Phone: (802)827-4513 Contracting Officer (CO) Charles (Charley) Julian Email: Charles.E.Julian@uscis.dhs.gov Phone: (802)872-4667 The total amount of award: $13,186,606.00. The obligation for this award is shown in box 26.				

Section B—Line Item Structure

			Base Period*							
Item	*CLIN type*	*Description*	*Qty Unit*		Base Period x = 0	*Qty Unit*		First Option Year x = 1	Second Option Year x = 2	Third Option Year x = 3
0001	FFP	Transition-IN *IAW PWS Section 5.*	1 MO	*unit price:* *amt:*	[redacted]					
x002	FFP	Agile Teams	1 LOT 11 MO	*unit price:* *amt:*	[redacted]	1 LOT POP 12 MO	*unit price:* *amt:*	[redacted]	[redacted]	[redacted]
x003	ODC	Government Directed Travel – Ref. H.6.1 of the EAGLE II Contract (NTE) *IAW PWS Section 7.4*	1 LO	*amt:*	$59,400			$59,400	$59,400	$59,400
			Total Base =		$5,133,898	***Total Option =***		[redacted]		
Total Value (Base and all Options): $ 13,186,606										

** CLIN 0001 will be the only CLIN billed during the one (1) month Transition-In period*

Section C—Task Order Clauses

Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.209-10 **Prohibition on Contracting With Inverted Domestic Corporations** (Nov 2015)

52.227-17 **Rights in Data—Special Works** (DEC 2007)

52.217-8 **Option to Extend Services** (Nov 1999)
fill-in: **30 days before the task order expires**

52.232-39 **Unenforceability of Unauthorized Obligations** (Jun 2013)

52.237-3 **Continuity of Services** (Jan 1991)

Federal Acquisition Regulation (FAR) clauses incorporated in full text

52.252-4 **Alterations in Contract** (Apr 1984)
Portions of this contract are altered as follows:

Use of the word "contract" is understood to mean "task order" wherever such application is appropriate. Use of the word "solicitation" is understood to mean "fair opportunity notice" wherever such application is appropriate.

52.203-99 **Prohibition On Contracting With Entities That Require Certain** (Jul 2016)

Internal Confidentiality Agreements (DEVIATION)

(a) The Contractor shall not require its employees or subcontractors seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the execution of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(b) The Contractor shall notify current employees and subcontractors that prohibitions and restrictions of any internal confidentiality agreements covered by this clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(d) In accordance with Section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235) use of funds appropriated (or otherwise made available) under that or any other Act may be prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(e) The Contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such contracts.

(f) The Government may seek any available remedies in the event the contractor fails to comply with the provisions of this clause.

52.217-9 **Option to Extend the Term of the Contract** (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within **15 days before the task order expires**; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **60 days** before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **54 months**.

Other Task Order Requirements

C-1. PAYMENT OF INVOICES

A "proper invoice" is defined under FAR Clause 52.232-25. Payment will be based on receipt of a proper invoice and satisfactory performance. Invoices shall be for approved expenses, such as travel, and services incurred during the previous month's period of performance.

Invoices shall be received within ten days following the end of the billing period, and shall include billable items for the previous month's period of performance. The contractor shall include with the invoice all supporting documents (e.g., travel reports/receipts) and the associated PER.

ADDITIONAL INVOICING INSTRUCTIONS

(a) In accordance with FAR Part 32.905, all invoices submitted to USCIS for payment shall include the following:

(1) Name and address of the contractor.
(2) Invoice date and invoice number.
(3) Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).
(4) Description, quantity, unit of measure, period of performance, unit price, and extended price of supplies delivered or services performed.
(5) Shipping and payment terms.
(6) Name and address of contractor official to whom payment is to be sent.
(7) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
(8) Taxpayer Identification Number (TIN).

(b) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.

(c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically to **USCISInvoice.Consolidation@ice.dhs.gov** with each email conforming to a size limit of 500 KB.

(d) If a paper invoice is submitted, mail the invoice to:

USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495
(802) 288-7600

(e) Each invoice shall include a table and illustrative graph for each cost-reimbursement CLIN showing the projected cost across the entire period of performance and the actual or incurred cost for every invoicing period to date.

C-2. PERFORMANCE REPORTING

The Government intends to record and maintain contractor performance information for this task order in accordance with FAR Subpart 42.15. The contractor is encouraged to enroll at www.cpars.gov so it can participate in this process.

C-3. HSAR CLAUSES INCORPORATED

HSAR clauses 3052.204-70 in section I.4.1 and HSAR clause 3052.204-71 in section I.4.2 of the parent EAGLE II Contract apply.

C-4. POSTING OF ORDER IN FOIA READING ROOM

(a) The Government intends to post the order resulting from this notice to a public FOIA reading room.

(b) Within 30 days of award, the Contractor shall submit a redacted copy of the executed contract (or order) (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The Contractor shall submit the documents to the USCIS FOIA Office by email at **foiaerr.nrc@uscis.dhs.gov** with a courtesy copy to the contracting officer.

(c) The USCIS FOIA Office will notify the contractor of any disagreements with the Contractor's redactions before public posting of the contract or order in a public FOIA reading room.

C-5. KEY PERSONNEL

For the purposes of the contract clause at HSAR 3052.215-70, Key Personnel or Facilities, the Key Personnel are listed in Section 4.1 in the Performance Work Statement (PWS).

C-6. NOTICE TO PROCEED (NTP)

(a) Performance of the work requires unescorted access to Government facilities or automated systems, and/or access to sensitive but unclassified information. The Attachment titled Security Requirements applies.

(b) The Contractor is responsible for submitting packages from employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A Government decision not to grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such decision or termination, shall not excuse the Contractor from performance of obligations under this task order.

(c) The Contractor may submit background investigation packages immediately following task order award.

(d) This task order does not provide for direct payment to the Contractor for EOD efforts. Work for which direct payment is not provided is a subsidiary obligation of the Contractor.

(e) The Government intends the Transition-In CLIN to begin **30 days** after task order award.

(f) The Government intends for full performance to begin **60 days** after task order award. The contracting officer will issue a notice to proceed (NTP) at least one day before full performance is to begin.

C-7. CONSENT TO SUBCONTRACT

For the purposes of the contract clause at FAR 52.244-2, Subcontracts, the fill-in for paragraph (d) is "ALL."

C-8. EXPECTATION OF CONTRACTOR PERSONNEL

The Government expects competent, production, qualified IT professionals to be assigned to the Agile Team. The Contracting Officer may, by written notice to the Contractor, require the contractor to remove any employee that is not found to be competent, productive, or qualified IT professional.

C-9. FINAL PAYMENT

As a condition precedent to final payment, a release discharging the Government, its officers, agents and employees of and from all liabilities, obligations, and claims arising out of or under this contract shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion as soon thereafter as practicable.

Section D—List of Attachments

Attch No.	Title	Number of Pages
1	Performance Work Statement (PWS)	17
2	Security Requirements	8
3	Capitalized Property, Plant & Equipment Assets Internal Use SW	8
4	Personal Identifiable Information (PII)	5
5	Accessibility Requirements (Section 508)	2

Performance Work Statement

Joint Engineering Teams – Sustainment of (JETS) Entity Analytics

1. Background

The Joint Engineering Teams Sustainment-Entity Analytics (JETS-EA) is a United States Citizenship & Immigration Services (USCIS) initiative spearheaded by the Office of Information Technology (OIT) Risk and Fraud Systems (RFS) Group. Its primary objective is to enhance operate and maintain the foundational Entity Analytics and Fraud Analysis services for the USCIS OIT and for the USCIS Fraud Detection and National Security (FDNS) directorate, in order to strengthen National Security safeguards and to enable USCIS to detect and combat immigration fraud.

1.0 Objective

The objective of this Performance Work Statement (PWS) is to obtain professional Information Technology (IT) services for the design, operation, maintenance, configuration, optimization and integration of Entity Analytics and Fraud Analysis software in support of FNDS efforts using the USCIS based infrastructure under USCIS Agile work patterns. The software and system is expected to operate in a standalone mode, as well as being able to operate in an integrated mode with USCIS systems such as FDNS-DS, ELIS and the USCIS Enterprise Services Bus (ESB). The supporting vendor will ensure the system is operational, as well as lead and perform Agile based development processes for the system, software, and supporting databases. The supporting vendor will serve as Big Data Entity Analytics and Fraud Analysis Subject Matter experts and as such provide USCIS with architectural knowledge on available platforms and systems and work to provide USCIS with options, plans, and recommendations on Entity Analytics and Fraud Analysis Capabilities.

2. Scope

The scope of the project includes the support of software installation, configuration, optimization and integration services in multiple USCIS software environments. USCIS currently uses IBM Identity Insight (ISII) and Global Name Recognition (GNR) in its Entity Analytics Capability. In conjunction with this task order, USCIS is researching and examining alternative solutions for Entity Analytics. The Contractor will provide key support in the examination process and support USCIS Entity Analytics with a dedicated and integrated team to provide services and will work with federal employees and other contractors in a scaled Agile approach to deliver high quality mission-based products in a responsive and cost effective manner. The Contractor shall be responsible for providing the proper level of personnel resources, as required, that are qualified and experienced in the following areas:

1) Project Management
2) Deployment, Operation, Enhancement, and Optimization of Entity Analytics Database

3) Deployment, Operation, Enhancement, and Optimization of Information Server, including associated software components such as InfoSphere DataStage and InfoSphere Data Replication (including CDC)

4) Deployment, Operation, Enhancement, and Optimization of the Entity Analytics Tool
5) Industry Wide available Data Analytics and Fraud Analysis Platforms and Systems and migration and transition plans and recommendations for USCIS use of these Platforms and Systems

This scope of work also includes the necessary privacy and security support to transition non-PII subsystems to PII based systems as required. It also includes all aspects of operating the system within the USCIS Infrastructure, including network integration and connections, firewall and security integration and connections, and processing and conducting USCIS Change and Release Management procedures. This is not simply a software coding and development effort, but a systems development, operations and maintenance engagement that will include efforts from across all of the IT disciplines required to operate the USCIS Entity Analytics Platform.

The Contractor shall be responsible for providing the proper level of personnel resources to support the development, operations and maintenance, effort for JETS EA. The development effort will be conducted using USCIS Agile Scrum practices. The Contractor should demonstrate knowledge and experience in efficient scrum practices, including all aspects of Sprint Releasing. USCIS expects an average of three to four week sprint cycles for EA releases, leading to 12-15 releases per year. The Contractor shall plan and practice releasing software that is fully tested, including integration and end-user, and that is fully documented and shippable.

The Contractor will also be responsible for leading and managing associated work to ensure the software can actually be released to production. This includes work such as connectivity between other systems, opening up firewalls, setting up databases and services, Data Center and Network coordination, Release and Testing documentation and other tasks beyond only software coding.

The approach of this task order is the Contractor will be the steward of the development, operations and maintenance of the EA system. A solution that just provides application development through the creation of software code for a portion of the EA system is not sufficient. The Contractor must be an integral part of the development, operations and maintenance of the EA platform within the USCIS infrastructure.

3 Specific Tasks

The Contractor shall provide professional IT services, under USCIS Kanban or other approved agile work patterns, for conducting the activities described in this PWS. In support of these activities, the Contractor shall be responsible for documenting its efforts in accordance with Section 6 of this PWS, and coordinated through the OIT Contracting Officer's Representative (COR), and USCIS OIT IT Project Manager (PM). Additionally, the Contractor shall assist with coordinating, monitoring, and managing the overall systems engineering lifecycle in conjunction with providing the services listed below:

- Application Program Management Service
    - Program Management
    - Subject Matter Expert

- Application Development Support Service
    - Application Development
    - Functional Analysis
    - Test Engineering Support
    - Project Management / Scrum Master support

The Contractor shall provide Program Management support for planning through delivery in accordance with USCIS approved Agile work patterns. While USCIS will provide Government oversight, it is the responsibility of the Contractor to manage all corporate resources and supervise all Contractor staff in the performance of all work on this task order. The Contractor shall assign a PM to manage the day-to-day activities of the Contractor staff. The PM shall have full responsibility for all deliverables.

Under this PWS, the Contractor will undertake the following activities:

Activity 1 - Project Management

The Contractor shall provide full time, dedicated project management support for planning through delivery in accordance with USCIS approved Agile work patterns. It is important to note the PM is to be fully responsible and authorized to lead, coordinate, and hold accountable all areas of the task order. While USCIS will provide Government oversight, it is the responsibility of the Contractor to manage all corporate resources and supervise all Contractor staff in the performance of all work on this task order. The Contractor shall assign a Project Manager (PM) who will manage the day-to-day activities of the Contractor staff. The PM shall have full responsibility for ensuring the delivery of all deliverables.

The Project Manager (PM) shall have full responsibility for all delivery items. The Project Manager shall organize, direct, and coordinate planning and execution of all task order activities, the review of all work, including subcontractors, to ensure that schedule, standards, and reporting responsibilities are met. The PM shall integrate the Contractor's management and technical activities across this task order to ensure they are consistent in terms of cost, schedule, scope, risk, issues, and quality. The PM shall ensure that all work complies with the terms and conditions of this task order. The PM shall be the primary interface with the USCIS CO, government PM, and COR. The PM shall attend daily, weekly, and monthly performance meetings and ad hoc meetings as required.

The purpose of this activity is to provide technical direction and control of the Contractor's project personnel and to provide a framework for project planning, communications, reporting and procedural activity. This activity is composed of the following tasks:

Planning

1) Review the PWS and the contractual responsibilities of both parties with the Government Project Manager.
2) Maintain project communications through the Government Project Manager.
3) Coordinate the establishment of the project environment.
4) Establish documentation and procedural standards for deliverables.

5) The Contractor will prepare and maintain the project plan in collaboration with the Government Program Manager for the performance of this PWS, which will include the product training plan, activities, tasks, assignments, milestones and estimates.

Project Tracking and Reporting

1) Review project tasks, schedules, and resources and make changes or additions, as appropriate. Measure and evaluate progress against the project plan with the Government Project Manager.
2) Work with the Government Project Manager to address and resolve deviations from the project plan.
3) Conduct regularly scheduled project status meetings.
4) Prepare and submit periodic Time Reports to the Government Project Manager.
5) Administer the Project Change Control Procedure with the Government Project Manager.
6) Coordinate and manage the technical activities of Contractor's team project personnel.

Deliverables:

- Project Plan
- Summary Report on Project Objectives
- Weekly and Monthly Status Reports
- Project Close-out Documentation

Activity 2 – Provide Entity Analytics and Fraud Analysis Subject Matter Expertise for Industry Wide Platforms and Systems

In this activity, the Contractor will perform services which include the following:

1) Review, analyze, and understand the existing USCIS Platform and Service
2) Review, analyze, plan, and make optimization and/or platform change recommendations based on available Industry-wide Entity Analytics and Fraud Analysis Software and Platforms
3) Provide overall migration recommendations, timeline, risks, plans, schedules, and decision points to USCIS based on tasks 1 and 2 above

Activity 3 – Support of the Deployment and Operation of the USCIS Entity Analytics

USCIS currently uses IBM DB2, Information Server, Identity Insight, Global Name Recognition, I2 Analyst's Notebook and I2 Analyze/IAP in its Entity Analytics Capability. USCIS is exploring alternative solutions and Entity Analytics Systems. The Contractor will support the current platform and participate, lead, and manage any migration to possible new alternative solutions.

The Contractor will operate, maintain, optimize, develop, enhance, and monitor the Entity Analytics System, using USCIS Agile Development Methodologies. This will include providing Tier 2 and Tier 3 level system administration, database administration, networking and O&M support.

Specific tasks include:

1) Maintain, install and configure the Entity Analytics System on multiple environments as required.
2) Ensure proper integration and connectivity between DB2, Identity Insight, IBM Global Name Management, Information Server and related software components, as well as with the sources of data ingested into the DB2 databases.
3) Test and validate on a continuing basis.
4) Complete and update installation documentation.
5) Perform system tuning for performance optimization as required.
6) Provide information security and privacy controls, with respect to system deployment, in accordance with the requirements specified by the *Security Requirements* section of this document.
7) Assess hardware/software environment; update and develop the installation plan as required, ensuring that it is current with respect to the state of the system's environments.
8) Conduct interviews with customer business organizations and technical teams to define and agree on overall business goals for the continued use of Entity Analytics.
    a. Establish well-articulated sets of use cases with business subject matter experts and data stewards. Update, modify, and upgrade existing use cases in accordance with new requirements.
    b. Develop strategies to incorporate use cases into daily business operations.
9) Own, work, and solve Entity Analytics System Trouble Tickets.
10) Participate and/or lead System Outage and Degradation Repairs, including the USCIS OIT Incident Response Team calls and meetings.
11) Respond to user training requests.
12) Answer operational issue questions.
13) Work jointly with other system owners and teams to ensure full integration and functionality of the overall availability of Entity Analytics systems.
14) Source Data Analysis
    a) For new data sources, assemble a data inventory of both accessible internal and obtainable external structured data, including purpose, format, volume, rate and method of refresh and potential correlation.
    b) Using data profiling tools such as, but not limited to, InfoSphere Discovery or InfoSphere Information Analyzer, analyze data sources to characterize data availability, integrity, density, variety, overlap, mapping, name and address presence and hygiene, data fidelity and transactional nature.
    c) Validate aggregate data source inputs and hardware sizing. This task applies to new data sources, and as required to existing data sources.
    d) Assign data cleansing priorities and responsibilities. This task applies to new data sources, and as required to existing data sources.

e) Establish feasible data remediation expectations. This task applies to new data sources, and as required to existing data sources.

f) Revise use cases as needed based on source system analysis and data profiling, for both existing and new data sources.

3.1 Agile Implementation of ESB and supported Services

The Contractor shall follow OIT approved Agile work patterns for implementation as it relates to the USCIS mission and RFS goals. The following outlines a typical OIT Kanban guideline.

3.1.1 Agile Team

The Contractor shall provide an Agile team able to maintain a two week Sprint Based Release Schedule.

The Contractor shall work as an Agile team, which *typically* includes the following roles:

- Product Owner(s) (PO) – Government Personnel
- Lead System Engineer (LSE) – Government Personnel
- Lead Business Representative (LBR) – Government Personnel
- Certified Scrum Master(s) (CSMs)
- Certified Developer(s)
- Certified Database Analyst(s)
- Business Analyst(s)
- Tester(s)

The Contractor shall provide all resources not identified as Government Personnel. In addition to the roles identified above, the Contractor shall provide the IT services as defined in this section under the guidance of stakeholders to include USCIS OIT management.

3.1.2 Release Schedule

The Contractor shall follow a Release schedule that is organized within USCIS approved Agile development guidelines. Specific release schedule details will be determined at the kickoff of the task order, with input from both contractor and government personnel.

3.1.3 Agile Meetings and Gate Reviews

The Contractor shall coordinate and lead the following meetings except for the Gate Reviews. For the Gate Reviews, the Contractor shall provide the required deliverables as noted below and respond to questions during the Review.

- System Engineering Division Engineering Change Control Board – provides approval to proceed.
- Release Planning Review (RPR) – *Gate Review*
- Planning and Grooming Meetings
- Product and Feature Demonstration Meetings
- Retrospective Meetings
- Release Readiness Review (RRR) – *Gate Reviews*

- Other meeting(s) as required by the Agile team to achieve Release goals (i.e. Daily Stand-up, backlog sessions, etc.)

3.1.4 Requirement/Development

The Contractor will participate and assist the Product Owners (PO) and SMEs to review the existing Product Backlog items as required. If there are no Product Backlog items or there is a higher priority to implement a new requirement not included in the Product Backlog, the Contractor shall elicit requirements and design for the new User Story.

Due to the nature of EA interfacing with multiple systems both internal and external to USCIS, the Contractor shall maintain active communication with the systems owners, development teams and business SMEs in order to capture complete requirements and dependencies.

3.1.5 Test, Evaluation and Security

The Contractor shall conduct all tests, evaluation, and security activities (e.g. unit, functional, integration, and acceptance tests) within the Agile team to ensure that the Services are functional and meet all Acceptance Criteria. The test, evaluation, and security activities of Services shall require the Contractor to closely coordinate with current system owners of interfacing systems, both internal and external to USCIS, throughout Release cycles. The Contractor shall provide results of the test as it relates to the defined Acceptance Criteria for each of the User Stories as a deliverable.

In accordance with the Agile process, a unified testing with the Independent Test Team is envisioned. The Contractor shall provide support for USCIS OIT Independent Test & Evaluation (IT&E) activities by inviting the IT&E resource to the Agile team's daily stand-up calls and other project meetings. The Contractor shall also invite the IT&E resource to witness the test activities within the Agile team and assist in demonstrating that all the Acceptance Criteria are met. If it is determined that additional testing, evaluation, or security activity is required for the Services, then the Contractor shall provide the necessary support to successfully conduct such activity.

3.1.6 Deliverable Documents

The Contractor shall deliver the following documents, in line with the Agile Development process scaled to fit USCIS missions.

- Gate Review Presentations
- System Design Document (SDD)
- Interface Control Agreement (ICA)

The Contractor shall assume and take over the management of existing Product Backlog for the existing EA Service using the Agile process. These documents should be accessible to anyone, (including, OIT management and Independent Test teams), on the USCIS OIT SharePoint at any given time during the release cycle. In addition to the deliverable documents, the Contractor shall maintain transparency of the release status by displaying the burn-down chart with the Government directed Agile Lifecycle Management medium.

4 Skillsets and Key Personnel

The Contractor shall provide the following personnel to meet the requirements of this task order. The personnel proposed shall possess the required education and experience to perform under this task order.

4.1 Key Personnel

The Contractor shall ensure the project is staffed with an adequate number of personnel possessing the required certifications, qualifications, skills and experience. The Contractor shall identify key personnel and provide statements of qualifications for these individuals. Key personnel shall be current, full time employees; contingent hires will not be accepted as key personnel submissions. The Contractor shall identify key personnel that shall be the **management lead** and the **technical lead** for the task order as a whole. These individuals must have expertise in the Agile development methodology. The Management Lead shall ensure that all work on this task order complies with task order terms and conditions, and shall have access to contractor corporate senior leadership when necessary. The Contractor's Management Lead shall be the primary interface with the COR and the CO, and shall attend status meetings and ad hoc meetings with stakeholders as required, accompanied by the Technical Lead when necessary.

Role	Labor Category	Certification	Experience
Program Manager	Program Manager	(PMP) Project Management Professional from the Project Management Institute or equivalent Project Management Certification.	Minimum of 7 years Program Management experience. Full oversight of the contract and its execution. Primary interface with COR, CO, IT PM and other stakeholders as needed.
Senior Technical Leader and Technology Consultant	Solutions Architect	NA	Experience with the suite of software products mentioned in the Scope section of the PWS, and in Activity 3 of the specific Tasks section. This suite includes InfoSphere Identity Insight, Global Name Recognition, Information Server, I2 Analyst's Notebook and I2 Analyze/IAP, and DB2. Experience with other Large Data Base Management Systems, and/or third party Data Base Management and Optimization Systems and Toolsets. Experience with integration frameworks which allow the building of complete entity resolution and analytics application pipelines. Experience with entity resolution and analytics software beyond the product suite mentioned in Activity 3 of the Specific Tasks section. The Senior Technology Consultant will also act as a technical team leader.

Role	Labor Category	Certification	Experience
Project Manager / Scrum Master	Project Manager	Certified SCRUM Master (CSM) Certification from Scrum Alliance or the equivalent.	Minimum of 5 years of experience leading SCRUM teams, or the equivalent, on Agile Projects.

5 Transition Support

5.1 Transition In

In accordance with Agile principles, knowledge acquisition is expected to occur within the sprints and releases, and thus a formal transition-in plan is not required. Upon notice to proceed, the Contractor transition-in will begin with the first sprint or first release and proceed for one month.

5.2 Transition Out

Upon completion of this task order, the Contractor shall fully support the transition of the Contractor's work that is turned over to another entity, either government or successor offeror(s). The Contractor shall assist with transition planning and shall comply with transition milestones and schedule of events.

The Contractor shall be responsible for the implementation of the transition and application cutover activities. The transition shall cause no disruption in development services. To ensure the necessary continuity of services and to maintain the current level of support, USCIS may retain services of the incumbent Contractor for some, or all, of the transition period, as required.
The Contractor shall be responsible for the transition of all technical activities identified in this task order. As part of the transition, the Contractor shall be responsible for:

- Inventory and orderly transfer of all Government Furnished Property (GFP), to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information (GFI)
- Transfer of documentation currently in process
- Transfer of all software code in process
- Certification that all non-public DHS information has been purged from any Contractor-owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to participate in transition management team

The Contractor shall submit a Transition Out Plan at the direction of the government. The Transition Plan shall:

- Document the strategic approach
- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish milestones and schedules

- Establish activities
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Create bi-party or tri-party agreements
- Provide transition checklists

The Transition Out Plan shall be delivered 60 calendar days prior to the task order expiration date or, if directed by the government, 60 days prior to the end of each option period, unless otherwise directed by the government.

Transition support shall commence upon direction of the government. The incumbent Contractor will work with the new Contractor to provide knowledge transfer and transition support, as required by the COR and PM.

6 Deliverables

The primary deliverable of this task order is deployable application code. The Contractor shall deliver this code (in conformance with procedures established by the Integration and Configuration team) throughout the period of performance for integration with an existing codebase in preparation for deployment.

The Contractor shall submit electronic copies of document deliverables (indicated in the table below) to the CO and COR (and others as specified by the CO and/or COR) via e-mail in the format specified below. All document deliverables shall be made by close of business (COB), 4:30pm local time, Monday through Friday, unless stated otherwise.

All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two business days after notification of the presence of a virus.

6.1 Task Order Management Artifacts

The Contractor shall provide reports that support task order management, as described below:

- Performance and Expenditure Report (PER)
  The PER shall contain a narrative of the month's activities and resources expenditures:
  - Performance Summary
    The Performance Summary includes documenting any major risks and/or issues, any significant progress, and events. Progress and events include the delivery of documents, artifacts, and code. The summary should provide enough detail for the reader with only some familiarity with the task order, to comprehend the value that the Contractor is providing to the overall application development effort at USCIS.
    Included with this summary shall be burn-down charts for those releases and iterations that ended within the month, and a snapshot of the burn-down chart for all releases and iterations in progress on the last day of the PER reporting period.

- Resource Expenditures
  Resource expenditures reports track funds expended during the reporting period and their purpose, in order to understand the burn rate and provide fiscal accountability to external stakeholders. Reporting of resource expenditures shall conform to the format provided in Attachment 3, Capitalized PP&E Assets IUS.

- Service Desk Report
  The Service Desk Report describes the Tier 2 and 3 service-desk tickets that the Contractor received (along with tracking number) for each Risk and Fraud Portfolio application, and classifies the defects into useful categories, such as defect or error, user knowledge or skills deficit, or an application usability issue. This report also shall recommend System Change Requests (SCR) in response to defects or other items as appropriate. The report shall show trends in the classification areas, and summarize cumulative monthly report data, as well as provide more detailed reporting of new items each month.

- Status Briefings
  As required by the COR, the Contractor shall attend meetings with the COR and/or other USCIS stakeholders in order to review work accomplished, work in progress, plans for future work, transition plans and status, and issues pertinent to the performance of work tasks that require USCIS attention. The meetings may be scheduled regularly or may be ad-hoc.

6.2 Deliverables Schedule

The deliverables that apply to this task order and that the Contractor shall provide are outlined in the table below.

Deliverables	Description	Frequency of Delivery	Acceptable formats
Key Personnel Statements of Qualification	Statements of Qualification in accordance with PWS Section 4.1	Within 5 days after task order award	Email to Contracting Officer
Kick Off Meeting Presentation	Presentation by Contractor consisting of a company overview, introduction of key personnel, company point of contact information for Security, Project Management, briefing of technical proposal, Invoicing, and questions and answers.	10 business days after Task Order award at USCIS OIT HQ	PowerPoint presentation
Program and Expenditure Report (PER)	Internal Use Software documentation in the format prescribed by OCFO to ensure that OIT is always in compliance	10th calendar day of each month	MS Word 2010, Excel

Deliverables	Description	Frequency of Delivery	Acceptable formats
Monthly Status Meeting	Monthly Status Reports, Project plans/updates, Invoices, and IUS documentation in the format prescribed by OCFO to ensure that OIT is always in compliance.	30 Days after award and monthly, by the 10th of each month, thereafter	PowerPoint
Status Briefing, such as presentations, database extractions, meeting reports, burndown charts, etc.	Power Point Presentation by Contractor.	30 Days after award and Monthly, by the 10th of each month, thereafter	MS Word 2010, Excel, Visio, or PowerPoint
Certification and Accreditation (C&A) documentation, Information Security Plan (ISP), contingency plans, disaster recovery plans, continuity of operations plans.	Applications Certification and Accreditation (C&A) Support	Within 30 days after award	MS Word 2010
Documentation to demonstrate maintenance of applicable items in the USCIS electronic document library, and compliance with a standard and accessible change control process in accordance with USCIS OIT CCRM policy.	Change, Configuration and Release Management (CCRM)	In accordance with (IAW) Approved Project Plan	
In-process application code	All the application code should be checked into USCIS approved continuous integration tool(s)	Continuously, with each build	Application source code
Shippable application code	All the application code should be checked into USCIS approved continuous integration tool(s)	Continuously, with each commit	Application source code and compiled code
Update documents such as: Quality Management Plan Test & Evaluation Management Plan Configuration	As required by USCIS IV &V team	Within 30 days after award; Updated annually thereafter or as required by the USCIS IV&V team processes	MS Word 2010

Deliverables	Description	Frequency of Delivery	Acceptable formats
Management Plan **Risk Management Plan** **Data Management Plan**			
Agile development lifecycle documents, such as System Design Document (SDD), User requirements definition, etc.	All the documentation as directed by USCIS IV&V and USCIS CCRM policies	As directed by USCIS IV&V for each new effort, release and/or deployment based on the latest policies and templates	MS Word 2010, MS Excel 2010, MS PowerPoint 2010
Transition Out Plan	Transition Out plan as described in PWS Section 5	60 calendar days prior to the task order expiration date or as directed by the government (IAW PWS Section 5).	MS Word 2010
Redacted copy of the executed task order including all attachments	Copy of the task order suitable for public posting under the provisions of the Freedom of Information Act (FOIA)	Within 30 days of task order award	Email to foiaerr.nrc@uscis.dhs.gov with a courtesy copy to the CO.
Separation Notification	The CO and COR must be notified of each contract employee termination/ resignation (The COR will then notify the Office of Security & Integrity (OSI) Personnel Security Division (PSD) to coordinate the exit clearance forms).	Within five (5) days of each occurrence.	E-mail

6.3 Inspection and Acceptance

Various government stakeholders will inspect Contractor services and deliverables. The CO will provide official notification of rejection of deliverables. Inspection and acceptance of deliverables will use the following procedures:

- The government will provide written acceptance, comments, and/or change requests, if any, within fifteen (15) business days of receipt of task order deliverables.
- Upon receipt of the government comments, the Contractor shall, within three (3) business days, rectify the situation and re-submit the task order deliverable(s).

7 Task Order Administration Data

7.1 Place of Performance

The principal place of performance shall be at the Contractor provided work site. The off-site Contractor facility shall be in close proximity to the USCIS facility at 111 Massachusetts Ave NW, Washington D.C, not to exceed a distance of 25 miles. Meetings will usually take place at USCIS offices in the Washington, D.C. Metropolitan Area, including, but not limited to, 20 Massachusetts Avenue, N.W., and 111 Massachusetts Avenue, N.W., Washington DC.

7.2 Hours of Operation

Normal duty hours will be 8:00am to 5:00pm, Eastern Standard Time (EST), Monday through Friday, excluding Government holidays, and will be based on a forty (40) hour work week.

7.3 Government Furnished Property (GFP)

Only GFP computers (including all normal forms of computing devices) will be issued and used in performing work on this task order. No personal or company owned storage devices, (thumb drives, DVDs, or CDs), shall be used with the GFP.

Equipment / Government Property	Date / Event Indicate when the GFP will be furnished	Date / Event Indicate when the GFP will be returned	Unit	Unit Acquisition Cost	Quantity	Serial Number(s)	Manufacture & Model Number	"As-Is"
Laptop computer with power cord, and desk lock	After EOD	Upon Departure	EA	$1,700	TBD	TBD	Standard USICS approved manufacturer	TBD
PIV Card	After EOD	Upon Departure	EA	$500	TBD	-	Standard USCIS approved manufacturer	TBD

Non GFP monitors, keyboards, mouse, and other non-computing peripherals may be used by the Contractor if desired by the Contractor. The government does not intend to provide non-computing peripherals.

The Contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation or rehabilitation costs. The Contractor will be responsible for receipt, stewardship, and custody of the listed GFP until formally relieved of responsibility in accordance with FAR 52.245-1 *Government Property* and FAR 52.245-9 *Use and Charges.* The property may not be used for any non-task order purpose. The Contractor bears full responsibility for any and all loss of this property, whether accidental or purposeful, at full replacement value.

7.4 Travel

Travel within the local commuting area will not be reimbursed. For the purpose of this task order, the local commuting area is defined as a fifty (50) mile radius from USCIS offices located at 111 Massachusetts Ave NW, Washington D.C. Home to work travel is not reimbursable. For this task order, the government will not pay travel for the Contractor to attend meetings in person at USCIS Offices in Washington DC. The only reimbursable travel planned under this task order will be for

Government determined, approved and directed onsite travel to USCIS Facilities outside of the Washington DC local commuting area.

8 Performance Criteria

The JETS-EA Contractor team will be evaluated monthly. The evaluation will be discussed with the Contractor. The purpose of the scorecard below and discussions is to enhance performance. In addition, in the aggregate, the scorecards and discussions will be used partially as a basis for past performance reporting. It is anticipated that the JETS-EA Contractor will be evaluated along the following dimensions:

No.	Performance Requirement	Performance Standard	Method of Measurement	Performance Metrics
1	Code Quality and Standards Adherence	Code will be evaluated against standards published by USCIS, including design standards and architecture.	Contractor code will be evaluated by Government teams and IV&V providers. Code will be evaluated against standards published by USCIS, including design standards and architecture. Automated code review tools will also be used to validate code quality.	**IDEAL:** Target level of defects free code for each software release deployed to production is 100%. **Acceptable:** Target level of defects free code for each software release deployed to production is 95%. **Not Acceptable:** Target level of defects free code for each software release deployed to production is less than 95%.
2	Business Satisfaction	Each feature completed by the Contractor team will be evaluated by the Government Product Owner for adherence to acceptance criteria as defined by the business Product Owner and SMEs assigned to the team.	The Contractor team will hold a functionality demonstration at the end of each sprint as Sprint Demo.	**IDEAL:** Target level of features free of defect and adhering to all the acceptance criteria is 100% **Acceptable:** Target level of features free of defects and adhering to critical acceptance criteria is 100% and adhering to the important acceptance criteria is 90% **Not Acceptable:** Target of features free of defects and adhering to less than 100% of critical acceptance criteria or adhering to the important acceptance criteria is less than 90%

3	Test Quality and Test Coverage	Each feature completed by the Contractor team will be evaluated against test coverage, (automation and manual test scripts), for all functional acceptance criteria.	Because automated tests are a key component of this process, test scripts will be treated as deliverables under JETS-EA. These test scripts will be assessed for their quality and for the extent to which they test the appropriate functions.	**Ideal:** All the acceptance criteria have 100% automation test coverage **Acceptable:** All functional acceptance criteria tested have a100% manual test coverage All functional acceptance criteria being regression tested have 100% automation coverage and at least 90% of new functional acceptance criteria have automation test coverage **Not Acceptable:** All the functional acceptance criteria being tested in the sprint do NOT have 100% manual test coverage and All the functional acceptance criteria being regression tested have less than 90% automation test coverage
4	Productivity	Each feature slated to be completed for the sprint should be complete as per the acceptance criteria listed and approved by the Product owner and other government SMEs as ready for production.	The Contractor team will present the Sprint Burn Up or Sprint Burn Down charts at the end of every sprint during the sprint retrospective. These charts will be used to evaluate the productivity of the team	**Ideal:** Target level of all the sprint features produced is 100% **Acceptable:** Target level of sprint features produced is 95% **Not Acceptable:** Target level of sprint features produced for less than 95%.

U.S. Citizenship and Immigration Services
Office of Security and Integrity – Personnel Security Division

SECURITY REQUIREMENTS

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees to government facilities and/or access of Contractor employees to sensitive but unclassified information based upon the results of a background investigation. USCIS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by USCIS, at any time during the term of the contract. No Contractor employee shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Office of Security & Integrity Personnel Security Division (OSI PSD).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the Position Designation Determination (PDD) for Contractor Personnel. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

To the extent the Position Designation Determination form reveals that the Contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the

following forms, in conjunction with security questionnaire submission of the SF-85P, "Security Questionnaire for Public Trust Positions" via e-QIP:

1. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"

2. FD Form 258, "Fingerprint Card" **(2 copies)**

3. Form DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

4. Position Designation Determination for Contract Personnel Form

5. Foreign National Relatives or Associates Statement

6. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)

7. ER-856, "Contract Employee Code Sheet"

EMPLOYMENT ELIGIBILITY

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the U.S. for three of the past five years, OSI PSD may not be able to complete a satisfactory background investigation. In such cases, USCIS retains the right to deem an applicant as ineligible due to insufficient background information.

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued by the Social Security Administration.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer's Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a contractor's reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than

December 31st each year, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on duty for new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **USCIS Office Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their own training)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire.

In accordance with Homeland Security Presidential Directive-12 (HSPD-12) http://www.dhs.gov/homeland-security-presidential-directive-12 contractor employees who require access to United States Citizenship and Immigration Services (USCIS) facilities and/or utilize USCIS Information Technology (IT) systems, must be issued and maintain a Personal Identity Verification (PIV) card throughout the period of performance on their contract. Government-owned contractor-operated facilities are considered USCIS facilities.

After the Office of Security & Integrity, Personnel Security Division has notified the Contracting Officer's Representative that a favorable entry on duty (EOD) determination has been rendered, contractor employees will need to obtain a PIV card.

For new EODs, contractor employees have [*10 business days unless a different number is inserted*] from their EOD date to comply with HSPD-12. For existing EODs, contractor employees have [*10 business days unless a different number of days is inserted*] from the date this clause is incorporated into the contract to comply with HSPD-12.

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:
http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx
Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.

Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing out so that it is visible at all times while in a USCIS facility
- Keep their PIV card current
- Properly store the PIV card while not in use to prevent against loss or theft http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OSI through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR and OSI shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COR determine that the Contractor is not complying with the security requirements of this contract the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

The Contractor shall be responsible for all damage or injuries resulting from the acts or omissions of their employees and/or any subcontractor(s) and their employees to include financial responsibility.

SECURITY PROGRAM BACKGROUND

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information*, August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004

- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal*
- *Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security*
- *Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor

employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.
CSAT can be accessed at the following: http://otcd.uscis.dhs.gov/EDvantage.Default.asp or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS and USCIS Policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN).* For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA):* This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A)**:*** This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features

and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self-Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY ASSURANCES

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

Security Clause 5 w/IT

DATA SECURITY

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling*. – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook*.

Security Clause 5 w/IT

Capitalized Property, Plant & Equipment (PP&E) Assets Internal Use Software (IUS)

1. Background

The United States Citizenship and Immigration Services Management Directive No. 128-001, USCIS/Office of Information Technology has an ongoing requirement to report Internal Use Software (IUS) costs for the programs under their purview and assignment. This report is a monthly mandatory requirement, and must include all software releases with a cumulative cost of $500K or greater; bulk purchases of $1 Million, and a useful life of 2 years or more.

2. Requirement

Reporting: All applicable charges for application releases and/or development charges are tracked and reported; documented by each applicable release so that an OIT determination can be made if the asset meets IUS criteria. USCIS has determined that the best method for identifying IUS candidates is through monthly collection of contractor cost data for all releases in development, and will capitalize the cost of an IUS project if it is classified as a G-PP&E asset and meets the required criteria.

Definition: IUS is software that is purchased from commercial off-the-shelf (COTS) vendors or ready to use with little or no changes. Internal developed software is developed by employees of USCIS, including new software and existing or purchased software that is modified with or without a contractor's assistance. Contractor-developed software is used to design, program, install, and implement, including new software and the modification of existing or purchased software and related systems, solely to meet the entity's internal or operational needs.

Invoicing and Reporting: The contractor shall identify, capture, log, track and report the costs of IUS associated with each specific release. IUS Software is typically release centric and includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program.

The contractor shall, after OIT's determination on whether or not the release meets the capitalization criteria, support OIT's reporting of costs incurred for the project or release, as required. The contractor shall provide the nature and cost of work completed within the relevant period. Costs considered part of IUS activities include systems administration, systems engineering, and program management. The Contractor shall provide the total cost, itemized by release and include the total sum of all applicable IUS activities (see sample format below).

For information purposes, the following activities within the development lifecycle have been identified as IUS reportable costs by the USCIS Management Directive No. 128-001:

a) Design: System Design: Design System, Update System Test Plan, Update Security Test Plan, Update Project Plan, Update Business Case, Conduct Critical Design Review and Issue Memo.
b) Programming/Construction: Establish Development Environment, Create or Modify Programs, Conduct Unit & Integration Testing, Develop Operator's Manual, Update Project Plan, Update Business Case, Migration Turnover/Test Readiness Review, Prepare Turnover Package, Develop Test Plans, Migration Turnover/Issue Test Readiness Memo

c) Testing
    i. Acceptance Testing: Develop Security Test Report, Issue Security Certification, Develop System Documentation, Conduct User Acceptance Testing, Update Project Plan, Update Business Case, Conduct Production Readiness Review, Develop Implementation Plan, Issue Production Readiness Review Memo.
    ii. Coding
    iii. Installation to hardware
    iv. Testing, including parallel processing phase
d) Implementation Activities: Implementation/Transition: Security Accreditation (initial system accreditation only), Issue Implementation Notice, Parallel Operations, Update Project Plans, Update Business Case, Conduct Operational Readiness Review, Issue Operational Readiness Memo.
e) In addition, these cost shall contain, if not already itemized in the attachment (PER) or the invoice, the following additional costs information: Full cost (i.e., direct and indirect costs) relating to software development phase; Travel expenses by employees/contractor directly associated with developing software; Documentation Manuals; COTS purchases.

The invoice shall include backup documentation in a format supplied by the Government. The Resource Expenditure Report and its associated Resource Expenditure Format constitute the invoice backup data that the Government requires. The invoice's Resource Expenditure Report shall follow the format provided in

Figure 1: Resource Expenditure Report. The contractor shall provide this in MS Excel format. A description of the data items in the report are provided in *Table 1: Resource Expenditure Format*. The report data shall represent the labor resources billed in the invoice. In other words, the amount billed shall be consistent with the resource expenditures documented for that reporting period. The Resource Expenditure Report reporting period shall be consistent with the invoices.

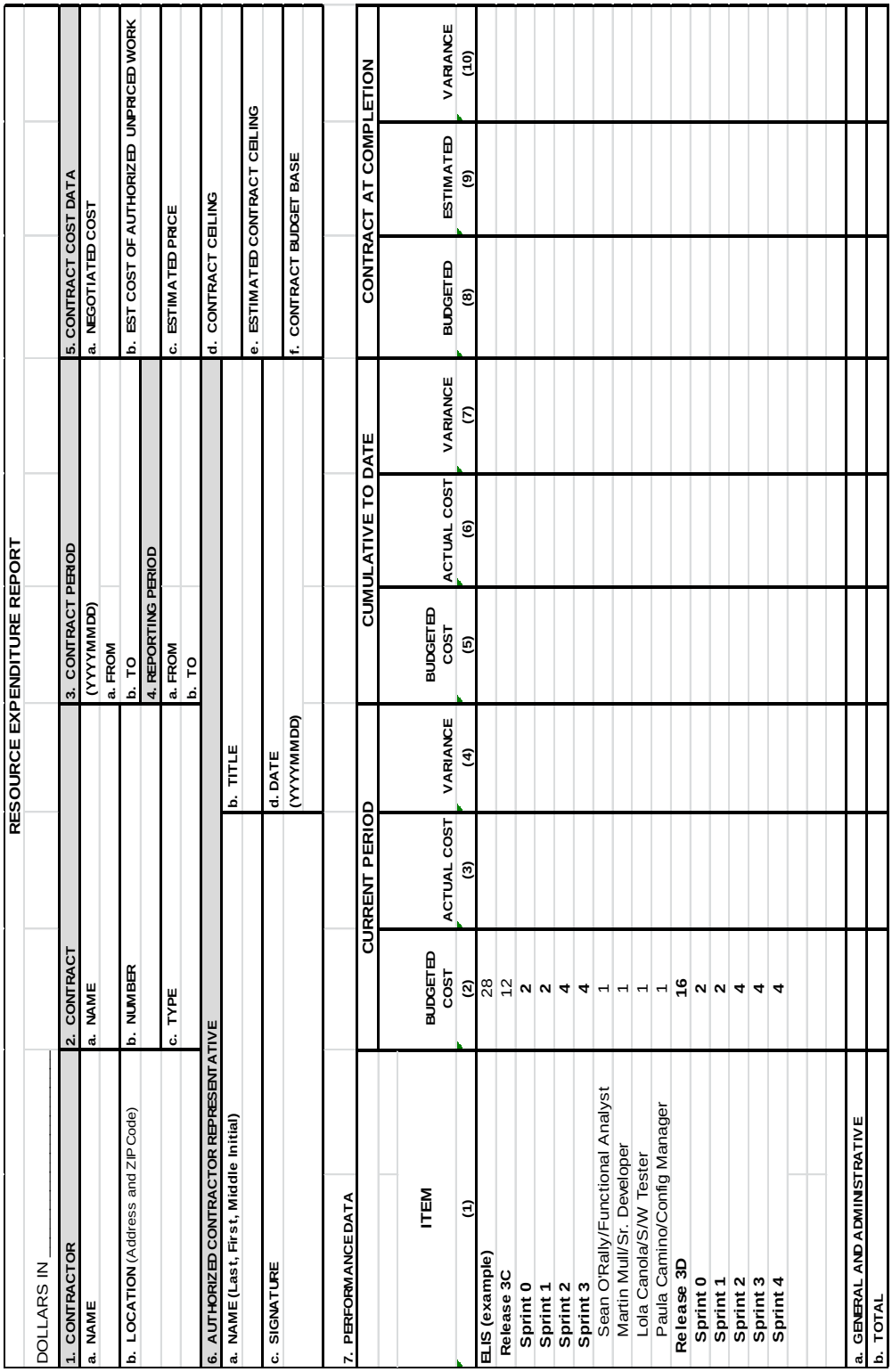
Table 1: Resource Expenditure Format

Item No.	Item	Description
1	Contractor	Enter the contractor name in (a) and the contractor facility address and mailing location in (b)
2	Contract	Enter the contract name in (a), the contract number in (b), and the contract type, such as T&M (c)
3	Contract Period	Enter the contract period of performance start and end dates
4	Reporting Period	Enter the start and end dates for the period covering the report
5a	Negotiated Cost	The dollar value (excluding fee or profit) on which the contractual agreement has been reached as of the cutoff date of the report. Amounts for changes shall not be included in this item until they have been priced and incorporated in the contract through contract change order or supplemental agreement.
5b	Estimated Cost of Authorized Unpriced Work	The amount (excluding fee or profit) estimated for that work for which written authorization has been received, but for which definitized contract prices have not been incorporated in the contract through contract change order or supplemental agreement.
5c	Estimated Price	Based on the most likely estimate of cost at completion for all authorized contract work and the appropriate profit/fee, incentive, and cost sharing provisions. Enter the estimated final contract price (total estimated cost to the Government). This number shall be based on the most likely management estimate at complete and normally will change whenever the management estimate or the contract is revised.
5d	Contract Ceiling	Contract ceiling price applicable to the definitized effort.
5e	Estimated Contract Ceiling	The estimated ceiling price applicable to all authorized contract effort including both definitized and undefinitized effort.
5f	Contract Budget Base	Enter the total of negotiated cost (5.a) and estimated cost of authorized, unpriced work (5.b).
6	Authorized Contractor Representative	Enter the name of the authorized person (program manager or designee) signing the report in (a), enter that person's title in (b), and enter the date signed in (d). The authorized person shall sign in (c). Electronic signatures are encouraged.
7(1)	Item	Create rows and sub-rows of data that represent the following items in nested order: Application - The name of each of the applications the contractor supports, such as “ELIS”. All data in this row will be a roll-up of all costs associated with this application. Release - The nomenclature of each of the releases the contractor supports that is associated with the named application, such as “A2.1”. All data in this row will be a roll-up of all costs associated with this release. Iteration - The nomenclature that identifies each of the iterations the contractor is supporting as part of the named release, such as “Sprint 4”, “Sprint 5”, etc. All data in these rows will be a roll-up of all costs associated with the named iteration. Individual – The names of all of the individuals who charged or planning to charge to the contract during the named sprint, followed by their labor category, such as “Sean O’Rally /Functional Analyst”. All data in these rows will be itemized costs associated with the named resources for the given iteration. Resources may be placed in planning packages for future releases and iterations that have yet to be identified

		during the contract period of performance.
7(2)	Current Period Budget Cost	For the reporting time period, indicate the cost of planned resources based on the release and iteration planning closest to the start of the period of performance.
7(3)	Current Period Actual Cost	For the reporting time period, indicate the actual costs of all resources used.
7(4)	Current Period Variance	For the reporting time period, indicate the difference between the actual and planned costs in terms of dollars with the percent represented in parenthesis following the dollar figures, such as "-243,900 (-6%)".
7(5)	Cumulative Budget Cost	For the contract time period, indicate the cumulative cost of planned resources from the start of the contract to the end of the reporting period.
7(6)	Cumulative Actual Cost	For the contract time period, indicate the cumulative actual costs of all resources used.
7(7)	Cumulative Variance	For the contract time period, indicate the cumulative differences between the actual and planned costs in terms of dollars with the percent represented in parenthesis following the dollar figures, such as "-243,900 (-6%)".
8(8)	Contract at Completion Budgeted	Enter the budgeted cost at completion for the items listed in Column (1). This entry shall consist of the sum of the original budgets.
7(9)	Contract at Completion Estimated	Enter the latest revised estimate of cost at completion including estimated overrun/underrun for all authorized work.
7(10)	Contract at Completion Variance	Enter the difference between the Budgeted - At Completion in Column (8) and the Estimated – At Completion in Column (9).
7(11)	Month *x* Budget Cost	The data in Column (11) is maintained for each month during the contract period of performance. For the month represented, indicate the cost of planned resources.
7(12)	Month *x* Actual Cost	The data in Column (12) is maintained for each month during the contract period of performance. For the month represented, indicate the actual costs of all resources used.
7(13)	Month *x* Variance	The data in Column (13) is maintained for each month during the contract period of performance. For the month represented, indicate the difference between the actual and planned costs in terms of dollars with the percent represented in parenthesis following the dollar figures, such as "-243,900 (-6%)".
7(14)	Fiscal Year and Quarter Budgeted Cost	For the government fiscal year (Oct 1 to Sept 30) and for each of the 4 quarters in the fiscal year, indicate the cumulative cost of planned resources. This will be cumulative costs of the relevant monthly costs (Column 14) in the fiscal year and the fiscal quarters that fall within the contract period of performance. If the contract period of performance ends prior to the conclusion of a fiscal year (Sept. 30), then the contractor shall estimate all of the available months within the fiscal year, recognizing that no work is scheduled to be performed during some of those months.
7(15)	Fiscal Year and Quarter Actual Cost	For the fiscal year and for each of the 4 quarters in the fiscal year, indicate the cumulative actual cost of resources. This will be cumulative costs of the relevant monthly costs (Column 15) in the fiscal year and the fiscal quarters that fall within the contract period of performance. If the contract period of performance ends prior to the conclusion of a fiscal year (Sept. 30), then the contractor shall estimate all of the available months within the fiscal year, recognizing that no work is scheduled to be performed during some of those months.
7.a	General & Administrative	Enter the appropriate General and Administrative (G&A) costs. If G&A costs have not been included in the (Column (1)) costs, G&A shall be shown as an add entry in (Column (1)). If G&A costs have been included

		in the Column (1) costs, G&A shall be shown as a non-add entry here with an appropriate notation to that effect. For contracts that require CCDRs, contractors may also have to submit separate costs without G&A for the Column (1) elements on an exception basis if the Government specifies such a requirement in the CDRL. If a G&A classification is not used, no entry shall be made other than an appropriate notation to that effect.
7.b	Total	Enter the sum of the budgeted cost, actual costs, variances, and estimated costs and G&A.

Figure 1: Resource Expenditure Report



RESOURCE EXPENDITURE REPORT

DOLLARS IN _____

1. CONTRACTOR	2. CONTRACT	3. CONTRACT PERIOD	5. CONTRACT COST DATA
a. NAME	a. NAME	(YYYYMMDD)	a. NEGOTIATED COST
		a. FROM	
b. LOCATION (Address and ZIP Code)	b. NUMBER	b. TO	b. EST COST OF AUTHORIZED UNPRICED WORK
		4. REPORTING PERIOD	
	c. TYPE	a. FROM	c. ESTIMATED PRICE
		b. TO	
6. AUTHORIZED CONTRACTOR REPRESENTATIVE			d. CONTRACT CEILING
a. NAME (Last, First, Middle Initial)		b. TITLE	e. ESTIMATED CONTRACT CEILING
c. SIGNATURE		d. DATE (YYYYMMDD)	f. CONTRACT BUDGET BASE

7. PERFORMANCE DATA

ITEM	CURRENT PERIOD			CUMULATIVE TO DATE			CONTRACT AT COMPLETION		
	BUDGETED COST	ACTUAL COST	VARIANCE	BUDGETED COST	ACTUAL COST	VARIANCE	BUDGETED	ESTIMATED	VARIANCE
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
ELIS (example)	28								
Release 3C	12								
Sprint 0	2								
Sprint 1	2								
Sprint 2	4								
Sprint 3	4								
Sean O'Rally/Functional Analyst	1								
Martin Mull/Sr. Developer	1								
Lola Canola/S/W Tester	1								
Paula Camino/Config Manager	1								
Release 3D	16								
Sprint 0	2								
Sprint 1	2								
Sprint 2	4								
Sprint 3	4								
Sprint 4	4								
a. GENERAL AND ADMINISTRATIVE									
b. TOTAL									

	Aug-12			Sep-12			FISCAL YEAR 2012		Oct-12			Nov-12			Dec-12			FY 2013 QUARTER 1		FISCAL YEAR 2013
	BUDGETED COST (11)	ACTUAL COST (12)	VARIANCE (13)	BUDGETED COST (11)	ACTUAL COST (12)	VARIANCE (13)	BUDGETED COST (14)	ACTUAL COST (15)	BUDGETED COST (11)	ACTUAL COST (12)	VARIANCE (13)	BUDGETED COST (11)	ACTUAL COST (12)	VARIANCE (13)	BUDGETED COST (11)	ACTUAL COST (12)	VARIANCE (13)	BUDGETED COST (14)	ACTUAL COST (15)	BUDGETED COST (14)	ACTUAL COST (15)

SECURITY OF SYSTEMS HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT RESPONSE

Privacy Clause Requirements.

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), to access information that meet the definition of Personally Identifiable Information (PII) and/or Sensitive PII, set forth below. Accordingly, the Contractor will adhere to the following:

(a) Definitions.

"Breach" (may be used interchangeably with "Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, acquisition, and/or access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

"Personally Identifiable Information (PII)" as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States. Sensitive PII is a subset of PII which requires additional precautions to prevent exposure or compromise.

Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Personally Identifiable Information (Sensitive PII)" as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(1) Driver's license number, passport number, or truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status

(4) Financial information such as account numbers or Electronic Funds Transfer Information
(5) Medical Information
(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be "sensitive" depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but it is not sensitive.

(b) Systems Access. Work to be performed under this contract requires the handling of PII and/or Sensitive PII. The contractor shall provide USCIS access to, and information regarding systems the contractor operates on behalf of USCIS under this contract, when requested by USCIS, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with USCIS in assuring compliance with such requirements. USCIS access shall include independent validation testing of controls, system penetration testing by USCIS, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

(c) Systems Security. In performing its duties related to management, operation, and/or access of systems, owned and or operated by USCIS as well as by the contractor, containing PII and/or Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in Department of Homeland Security (DHS) Sensitive System Publication 4300A or any superseding publication, and Rules of Behavior.

In addition, use of contractor-owned laptops or other mobile media storage devices to include external hard drives and memory sticks to process or store PII/Sensitive PII is prohibited under this contract unless the Contracting Officer (CO) in coordination with the USCIS Chief Information Security Officer (CISO) approves. If approval is granted the contractor shall provide written certification that the following minimum requirements are met:

(1) Laptops shall employ full disk encryption using NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;

(2) Mobile computing devices use anti-viral software and a host-based firewall mechanism;

(3) When no longer needed, all mobile media and laptop hard drives shall be processed (i.e., sanitized, degaussed, and/or destroyed) in accordance with DHS security requirements set forth in DHS Sensitive System Publication 4300A. The USCIS reserves the right to audit random media for effectiveness of sanitization or degaussing. The contractor shall provide the requested equipment to USCIS no later than 15 days from the date of the request.

(4) The contractor shall maintain an accurate inventory of devices used in the performance of this contract and be made available upon request from USCIS;

(5) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the Contracting Officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

(d) Data Security. Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure PII/Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When PII/Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the PII/Sensitive PII irretrievable.

The contractor shall only use PII/Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the Contracting Officer. At expiration or termination of this contract, the contractor shall turn over all PII/Sensitive PII obtained under the contract that is in its possession to USCIS.

(e) Breach Response. The contractor agrees that in the event of any actual or suspected breach of PII/Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the Contracting Officer , the Contracting Officer's Representative (COR), and the USCIS Service Desk and complete an Incident Report with the Service Desk Representative. The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties. Email notification shall be used to document all telephonic notifications.

(f) Personally Identifiable Information Notification Requirement. The contractor will have in place procedures and the capability to promptly notify any individual whose PII/Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate by USCIS. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of USCIS, based upon a risk-based analysis conducted by USCIS in accordance with DHS Privacy incident Handling Guidance and USCIS Privacy Incident Standard Operating Procedures. Notification shall not proceed unless USCIS has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to USCIS analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by USCIS. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

The contractor agrees to assist in and comply with PII/Sensitive PII incident remediation and/or mitigation efforts and instructions, including those breaches that are not a result of the contractor or employee actions, but the contractor is an unintentional recipient of privacy data. Actions may include allowing USCIS incident response personnel to have access to computing equipment or storage devices, complying with instructions to remove emails or files from local or network drives, mobile devices (BlackBerry, Smart Phone, iPad, USB thumbdrives, etc…).

In the event that a PII/Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to USCIS, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should USCIS elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing USCIS for those expenses. To ensure continuity with existing government identity protection and credit monitoring efforts, the contractor shall use the identity protection service provider specified by USCIS.

(g) Privacy Training Requirement. The performance of this contract has been determined to have the potential of allowing access, by Offeror employees, to Personally Identifiable Information (PII) and/or Sensitive PII, which is protected under the Privacy Act of 1974, as amended at 5 USC §552a. The Offeror is responsible for ensuring all employees who have access to information protected under the Privacy Act complete annual mandatory USCIS Privacy Awareness Training. New Offeror employees shall complete PII training within 30 days of entry on duty. The Offeror shall use the USCIS provided web-based Privacy Training which is available through the USCIS LearningEdge training system http://learningedge.uscis.dhs.gov to satisfy this requirement. Any employees who do not have access to the online LearningEdge training system shall take Privacy training via a USCIS provided DVD. The Offeror shall certify as soon as this training is completed by its employees and annually thereafter on September 30th. The certification of the completion of the training by all employees shall be provided to both the COR and CO; within 60 days of contract award, within 45 days of new employee accession and no later than September 30th for the annual recertification.

(h) Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this

contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

(i) Ability to Restrict Access to Information. USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising Personally Identifiable Information (PII), Sensitive PII (SPII), Sensitive But Unclassified (SBU) information and/or classified information.

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. In addition, contractor personnel who support any aspect of user-interface development and testing shall become DHS OAST-certified Trusted Testers within 6 months of contract award. Specifically, the following applicable EIT accessibility standards have been identified:

1. Section 508 Applicable EIT Accessibility Standards

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

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

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

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

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

2. 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.

3. 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 thatmeet 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.