

# ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES


1 13

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

1. DATE OF ORDER 06/09/2017		2. CONTRACT NO. (If any) HSHQDC-13-D-E2075		6. SHIP TO: a. NAME OF CONSIGNEE Department of Homeland Security	
3. ORDER NO. HSSCCG17J00025		4. REQUISITION/REFERENCE NO.		b. STREET ADDRESS Citizenship & Immigration Services Chief Information Officer 5th floor #102 111 Massachusetts Ave NW	
5. ISSUING OFFICE (Address correspondence to) USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403				c. CITY Washington	d. STATE DC
				e. ZIP CODE 20001	
7. TO: a. NAME OF CONTRACTOR SEVATEC INC				f. SHIP VIA	
b. COMPANY NAME				8. TYPE OF ORDER <input type="checkbox"/> a. PURCHASE <input checked="" type="checkbox"/> b. DELIVERY	
c. STREET ADDRESS 3112 FAIRVIEW PARK DRIVE				REFERENCE YOUR: Sevatec Offer Dated December 2, 2016 Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.	
d. CITY FALLS CHURCH	e. STATE VA	f. ZIP CODE 220424504		Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.	
9. ACCOUNTING AND APPROPRIATION DATA See Schedule		10. REQUISITIONING OFFICE USCIS Contracting Office		12. F.O.B. POINT Destination	
11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM <input type="checkbox"/> h. EDWOSB					
13. PLACE OF a. INSPECTION Destination		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) Multiple	
b. ACCEPTANCE Destination				16. DISCOUNT TERMS Net 30	

## 17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 132599668+0000 Data and Business Intelligence Support Services (DBIS) III Continued ...					
18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h) TOTAL (Cont. pages)
21. MAIL INVOICE TO: a. NAME See Invoicing Instructions						
b. STREET ADDRESS (or P.O. Box)						17(i) GRAND TOTAL
c. CITY						
		d. STATE	e. ZIP CODE			

22. UNITED STATES OF AMERICA BY (Signature) 	23. NAME (Typed) James A. Boehm TITLE: CONTRACTING/ORDERING OFFICER
--	---

AUTHORIZED FOR LOCAL REPRODUCTION  
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 2/2012)  
Prescribed by GSA/FAR 48 CFR 53.213(f)

**ORDER FOR SUPPLIES OR SERVICES**  
**SCHEDULE - CONTINUATION**

PAGE NO  
2

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

DATE OF ORDER 06/09/2017	CONTRACT NO. HSHQDC-13-D-E2075	ORDER NO. HSSCCG17J00025
-----------------------------	-----------------------------------	-----------------------------

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	AAP Number: None DO/DPAS Rating: NONE Period of Performance: 06/12/2017 to 06/11/2021  POP: 06/12/2017 to 08/11/2017					
0001	Transition-In IAW PWS Section 4.1 FFP  Accounting Info: Funded: \$0.00  Base Period Full Performance POP: 08/12/2017 - 06/11/2018					
0002	eCISCOR and SMART Development  [REDACTED] [REDACTED] [REDACTED]  Accounting Info: VISMDRN 000 OS 70-01-00-000 07-20-0200-00-00-00-00 GE-25-76-00 000000 [REDACTED] Accounting Info: SVEMDRN 000 EX 60-01-00-000 07-20-0100-00-00-00-00 GE-25-76-00 000000 [REDACTED] Accounting Info: ITENTSR ECC EX 20-01-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 [REDACTED] Accounting Info: ITENTSR SMA EX 20-01-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 [REDACTED]					
0003	Operation and Maintenance (O&M) and End User Support eCISCOR and SMART FFP  Accounting Info: ITAPPIN LSS EP 20-05-00-000 Continued ...					















TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES**  
**SCHEDULE - CONTINUATION**

PAGE NO  
3

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

DATE OF ORDER 06/09/2017	CONTRACT NO. HSHQDC-13-D-E2075	ORDER NO. HSSCCG17J00025
-----------------------------	-----------------------------------	-----------------------------

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
0004	23-20-0500-00-00-00-00 GE-25-86-00 000000  Program Management IAW PWS Section 4.6 FFP  Accounting Info: SVEMDRN 000 EX 60-01-00-000 07-20-0100-00-00-00-00 GE-25-76-00 000000  Accounting Info: ITAPPIN LSS EP 20-05-00-000 23-20-0500-00-00-00-00 GE-25-86-00 000000 					
0005	Infrastructure Support IAW PWS Section 4.5       Accounting Info: ITAPPIN LSS EP 20-05-00-000 23-20-0500-00-00-00-00 GE-25-86-00 000000 					
0006	SAS Development and Support       Accounting Info: ITENTSR ECC EX 20-01-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000  Accounting Info: ITENTSR SMA EX 20-01-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000   Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES**  
**SCHEDULE - CONTINUATION**

PAGE NO  
4

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

DATE OF ORDER 06/09/2017	CONTRACT NO. HSHQDC-13-D-E2075	ORDER NO. HSSCCG17J00025
-----------------------------	-----------------------------------	-----------------------------

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
0007	Government Directed Travel - Ref. H.6.1 of the EAGLE II Contract (NTE) IAW PWS Section 5.5 ODC  Accounting Info: ITAPPIN LSS EP 20-05-00-000 23-20-0500-00-00-00-00 GE-25-86-00 000000 [REDACTED]  Option 1 POP: 06/12/2018 - 06/11/2019					
1002	eCISCOR and SMART Development  [REDACTED] [REDACTED] [REDACTED] [REDACTED] (Option Line Item) Anticipated Exercise Date:08/12/2017					
1003	Operation and Maintenance (O&M) and End User Support eCISCOR and SMART FFP [REDACTED] (Option Line Item) Anticipated Exercise Date:06/12/2018  Accounting Info: Funded: \$0.00					
1004	Program Management IAW PWS Section 4.6 FFP [REDACTED] (Option Line Item) Anticipated Exercise Date:06/12/2018					
1005	Infrastructure Support IAW PWS Section 4.5  [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Anticipated Exercise Date:06/12/2018 Continued ...	1				

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES**  
**SCHEDULE - CONTINUATION**

PAGE NO  
5

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

DATE OF ORDER 06/09/2017	CONTRACT NO. HSHQDC-13-D-E2075	ORDER NO. HSSCCG17J00025
-----------------------------	-----------------------------------	-----------------------------

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
1006	SAS Development and Support  [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Anticipated Exercise Date:06/12/2018					
1007	Government Directed Travel - Ref. H.6.1 of the EAGLE II Contract (NTE) IAW PWS Section 5.5 ODC [REDACTED] Anticipated Exercise Date:06/12/2018  Option 2 POP: 06/12/2019 - 06/11/2020					
2002	eCISCOR and SMART Development [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Anticipated Exercise Date:08/12/2019					
2003	Operation and Maintenance (O&M) and End User Support eCISCOR and SMART FFP [REDACTED] [REDACTED]m) Anticipated Exercise Date:06/12/2019  Accounting Info: Funded: \$0.00					
2004	Program Management IAW PWS Section 4.6 FFP [REDACTED] [REDACTED] Anticipated Exercise Date:06/12/2019  Continued ...					



















TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES**  
**SCHEDULE - CONTINUATION**

PAGE NO  
6

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

DATE OF ORDER 06/09/2017	CONTRACT NO. HSHQDC-13-D-E2075	ORDER NO. HSSCCG17J00025
-----------------------------	-----------------------------------	-----------------------------

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
2005	Infrastructure Support IAW PWS Section 4.5      Anticipated Exercise Date:06/12/2019					
2006	SAS Development and Support      Anticipated Exercise Date:06/12/2019					
2007	Government Directed Travel - Ref. H.6.1 of the EAGLE II Contract (NTE) IAW PWS Section 5.5 ODC  Anticipated Exercise Date:06/12/2019  Option 3 POP: 06/12/2020 - 06/11/2021					
3002	eCISCOR and SMART Development      Anticipated Exercise Date:08/12/2020					
3003	Operation and Maintenance (O&M) and End User Support eCISCOR and SMART FFP   Anticipated Exercise Date:06/12/2020 Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES**  
**SCHEDULE - CONTINUATION**

PAGE NO  
7

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

DATE OF ORDER 06/09/2017	CONTRACT NO. HSHQDC-13-D-E2075	ORDER NO. HSSCCG17J00025
-----------------------------	-----------------------------------	-----------------------------

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
3004	Accounting Info: Funded: \$0.00  Program Management IAW PWS Section 4.6 FFP [REDACTED] [REDACTED] Anticipated Exercise Date:06/12/2020					
3005	Infrastructure Support IAW PWS Section 4.5 [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Anticipated Exercise Date:06/12/2020					
3006	SAS Development and Support [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] Anticipated Exercise Date:06/12/2020					
3007	Government Directed Travel - Ref. H.6.1 of the EAGLE II Contract (NTE) IAW PWS Section 5.5 ODC [REDACTED] Anticipated Exercise Date:06/12/2020  The following are the points of contact for this contract:  Contracting Officer's Representative (COR): Silvia A. Whitenack Phone: (202) 272-8223 Email: Silvia.A.Whitenack@uscis.dhs.gov COR Invoice Delegation: Recommend Approval of Invoices  Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

ORDER FOR SUPPLIES OR SERVICES  
SCHEDULE - CONTINUATION

PAGE NO  
8

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
06/09/2017	HSHQDC-13-D-E2075	HSSCCG17J00025

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	<p>Contracting Specialist (CS): Corinne G. Carmona Phone: (802) 872 - 4135 Email: Corinne.G.Carmona@uscis.dhs.gov</p> <p>Contract Officer (CO): James A. Boehm Phone: (802) 872 - 4164 Email: James.A.Boehm@uscis.dhs.gov</p> <p>The total amount of award: [REDACTED] The obligation for this award is shown in box 17(i).</p>					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))



## Section C—Task Order Clauses

### Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.209-10	<b>Prohibition on Contracting With Inverted Domestic Corporations</b>	(Nov 2015)
52.215-13	<b>Subcontractor Certified Cost or Pricing Data—Modifications</b>	(Oct 2010)
52.227-14	<b>Rights in Data—General Alternate III</b>	(May 2014) (Dec 2007)
52.232-39	<b>Unenforceability of Unauthorized Obligations</b>	(Jun 2013)
52.252-6	<b>Authorized Deviations in Clauses</b>	(Apr 1984)
	fill-in: <u>52.203-99 Prohibition On Contracting With Entities That Require Certain Internal Confidentiality Agreements (Jul 2016)</u>	

### Federal Acquisition Regulation (FAR) clauses incorporated in full text

52.203-99	<b>Prohibition On Contracting With Entities That Require Certain Internal Confidentiality Agreements</b>	(Jul 2016)
	<p>(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).</p> <p>(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.</p> <p>(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.</p> <p>(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.</p> <p>(e) The Contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such contracts.</p> <p>(f) The Government may seek any available remedies in the event the contractor fails to comply with the provisions of this clause.</p> <p>(Deviation)</p>	
52.252-4	<b>Alterations in Contract</b>	(Apr 1984)
	<p>Portions of this contract are altered as follows:</p> <p><u>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.</u></p>	
52.217-9	<b>Option to Extend the Term of the Contract</b>	(Mar 2000)
	<p>(a) The Government may extend the term of this contract by written notice to the Contractor within <u>30 days before the task order expires</u>; provided that the Government gives the Contractor a</p>	

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 **48 months**.

### Other Task Order Requirements

#### C-1. 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) All written approvals for travel shall be included with the submitted invoice.

(f) 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](http://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](mailto: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 5.4 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 **60 days** after task order award.

(f) The Government intends for full performance to begin **120 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.

(g) The Government reserves the right to withhold payment or take other the appropriate action if the Contractor is not prepared to begin full performance 120 days after task order award.

**C-7. CROSS CLIN BILLING**

The contractor shall not include any hours under a cost-reimbursement CLIN for an employee performing under a fixed price CLIN.

**C-8. PAYMENT OF FIXED FEE**

(a) For the purposes of the contract clause at FAR 52.216-8, Fixed Fee, payment of the fixed fee shall be made as specified below:

- 20% of the fixed fee when the period of performance is one-fourth complete;
- 20% of the fixed fee when the period of performance is one-half complete;
- 20% of the fixed-fee when the period of performance is three-fourths complete; and
- 40% of the fixed fee when the period of performance is complete.

(b) The contracting officer withholds a reserve of the fee contemplated by paragraph (b) of the clause at FAR 52.216-8 shall be deducted from the amounts shown above.

**C-9. LIMITATION OF FUNDS REPORTING ON CLIN BASIS**

For the purposes of the contract clause at FAR 52.232-22, Limitation of Funds, the requirement for a contractor notice in paragraph (c) of the clause applies at the CLIN level.

**C-10. 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-11. PAYMENT FOR OVERTIME PREMIUMS ON COST CLINS**

For the purposes of the contract clause at FAR 52.222-2, the fill-in for paragraph (a) is "ZERO."

**Section D—List of Attachments**

Attch

No.    Title

1	Performance Work Statement (PWS)	35
2	Security Requirements	8
3	IT Security Language	5
4	Personal Identifiable Information (PII)	5

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES



## Performance Work Statement

---

# Data and Business Intelligence Support Services (DBIS) III

**Office of Information Technology (OIT)**

**6/9/2017**

## CONTENTS

1.	Mission .....	3
1.1.	USCIS Mission .....	3
1.2.	DBIS Mission .....	3
2.	Objective and Scope .....	5
2.1.	Objective .....	5
2.2.	Scope .....	5
3.	Current State .....	6
3.1.	DBIS Existing Technology Stack and tools .....	6
3.2.	Agile Analytics Approach .....	7
3.3.	enterprise Citizenship & Immigration Services Centralized Operational Repository (eCISCOR) .....	7
3.4.	Standard Management Analysis Reporting Tool (SMART) .....	8
3.5.	SAS Predictive Modeling Environment (SAS PME) .....	9
4.	Tasks .....	11
4.1	Transition-In .....	11
4.2.	System Development .....	11
4.2.1	Emerging Technologies Development .....	11
4.2.2	eCISCOR Development .....	12
4.2.3	BI Development .....	15
4.2.4	SAS Development .....	15
4.2.5	Testing and Evaluation Support .....	16
4.2.6	Configuration Management and System Security Posture .....	16
4.3.	Operations and Maintenance (O&M) .....	17
4.3.1.	O&M - eCISCOR .....	17
4.3.2.	O&M - SMART .....	18
4.3.3	O&M - SAS .....	18

4.4.	End User Support and Change Management .....	19
4.4.1.	Systems Issue Intake .....	19
4.4.2.	Training Development and Delivery .....	19
4.5	Infrastructure Support .....	21
4.5.1	eCISCOR Database Infrastructure support .....	22
4.5.2	ETL Administration .....	22
4.5.3	SAS Administration.....	23
4.5.4	OBIEE Administration .....	23
4.6	Program Management .....	24
4.7	Transition-Out .....	25
5.	Task Order Administration .....	26
5.1.	Deliverables .....	26
5.2.	Schedule of Deliverables .....	26
5.3.	Place of Performance .....	29
5.4.	Key Personnel.....	30
5.5	Government-Directed Travel .....	32
5.6	Government Furnished Property .....	33
5.7	Government Furnished Information .....	33
5.8	Hours of Operation .....	35
5.9	Telework.....	35



# Performance Work Statement

## Data and Business Intelligence Support Services (DBIS III)

### 1. MISSION

#### 1.1. USCIS MISSION

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is responsible for lawful immigration to the United States. USCIS secures America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system.

USCIS has 18,000 Government employees and Contractors working at 250 offices worldwide. USCIS' strategic goals include:

- Strengthening the security and integrity of the immigration system
- Providing effective customer-oriented immigration benefit and information services
- Supporting immigrants' integration and participation in American civic culture
- Promoting flexible and sound immigration policies and programs
- Strengthening the infrastructure supporting the USCIS mission
- Operating as a high-performance organization that promotes a highly talented workforce and a dynamic work culture

#### 1.2. DBIS MISSION

DBIS is a program under the Systems Development Division (SDD), Office of Information Technology (OIT), Management Directorate.

To support the above mission of USCIS, the agency needs to have complete oversight of all aspects of its operations, which is mainly supported by the DBIS program through the implementation of operational and analytical reports and data sharing via several Information Technology (IT) systems. The mission of DBIS is two-fold:

- Provide reporting capability, which includes ad-hoc reporting, canned reports, and analytical capabilities via dashboards, data visualization, and statistical analysis

- Provide access to data for interconnected systems that ingest data from other systems for operational use via data service Application Programming Interfaces (APIs), web services, or other methods mutually agreed upon

Currently DBIS provides these capabilities via its three (3) system components:

- The enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR) - eCISCOR is a collection of databases that houses the agency's data in relational and dimensional data model format
- Standard Management Analytics and Reporting Tools (SMART) - SMART is an Oracle Business Intelligence Enterprise Edition (OBIEE) commercial product and provides access to data stored in eCISCOR for the purposes of operational and analytical reporting and analysis
- SAS <sup>®1</sup> – a commercial product of the SAS Institute. Provides access to data stored in eCISCOR for the purposes of business intelligence reporting, statistical analysis, statistical modeling and forecasting

---

<sup>1</sup> Formally known as Statistical Analysis Software

## 2. OBJECTIVE AND SCOPE

### 2.1. OBJECTIVE

The objective of this Performance Work Statement (PWS) is to obtain professional IT services to provide the design, architecture, configuration, development, and maintenance of the existing technological solution and enhancement of the analytical capabilities of USCIS by evolving the legacy environment with 21<sup>st</sup> century technologies, such as data visualization, no- SQL (Structured Query Language) querying, data analytics for decision-making, big data, open source tools, and data science. Throughout the duration of this task order, the Contractor will be expected to develop new capabilities by bringing in new data into the data repository from USCIS transactional systems, develop dimensional data models for business-function-specific data marts that will provide for cross-mart reporting, and develop new reports, dashboards, and ad-hoc reporting capabilities in various analytical tools. The Contractor will be expected to maintain all previously developed systems capabilities, maximize usage of the tools procured by the Government, provide training for the user community on existing and new tools, maintain system infrastructure, and provide proper program management and support.

### 2.2. SCOPE

This task order will be the primary vehicle to obtain professional IT architectural, systems development, and systems support services to continue the transformation of data from the USCIS transactional systems into a state-of-the-art enterprise data warehouse and associated operational and Business Intelligence (BI) reporting capabilities. The development scope of the program involves transforming agency-wide analytical capabilities and enhancing the agency's ability to use its large data pool for decision-making and operational improvement; any USCIS, DHS, or external federal agency system can become a source of data for DBIS, if dictated by the mission.

It is expected that throughout the execution of this task order the Government will invest in new tools and technologies that will further enhance DBIS capabilities in meeting its mission. Such transitions and new tools' implementation shall be supported by the Contractor.

The Government has decided to move the DBIS system components to the Cloud, which is currently being piloted. The task order work includes full support for the full move to the Cloud, which may include the complete re-architecture of the eCISCOR data repository and reporting and analytical capabilities. Furthermore, administration of all DBIS system components in the Cloud is within the scope of this task order.

USCIS reserves the right to change the strategic direction of the technical implementation of the task order. The task order work includes adapting to new and/or evolving technical approaches, as well as providing technical and program support to research, consult, and implement emerging technologies that the USCIS Chief Information Officer (CIO) deems appropriate to support the Agency's goals and objectives. Such shifts in the technical approach under the umbrella of the BI/Data Warehouse (DW) and data analytics are within the scope of this task order.

### 3. CURRENT STATE

#### 3.1. DBIS EXISTING TECHNOLOGY STACK AND TOOLS

The current set of infrastructure and tools, within which the task order Contractor must initially operate within, includes:

**Technical Stack:**

- Oracle 11G as the database platform (upgrade to 12c)
- OBIEE 11G – BI tool (upgrade to 12c)
- Informatica PowerCenter 9.5 (upgrade to v 10.1)
  - Informatica PowerExchange
  - Informatica Data Quality and Data Governance Enterprise edition (all included products)
- SAS® Enterprise, Version 9.4 – statistical tool
- Amazon Web Service (AWS)
  - Amazon Relational Database Services (RDS)
  - Amazon Elastic Compute Cloud (EC2)
  - Amazon Simple Storage Services (S3)
  - Amazon Glacier
  - Amazon RedShift
- Open source data analytics tools implemented in AWS based on a Software-as-a-Service architecture

**Agile Development and Project Management Tools:**

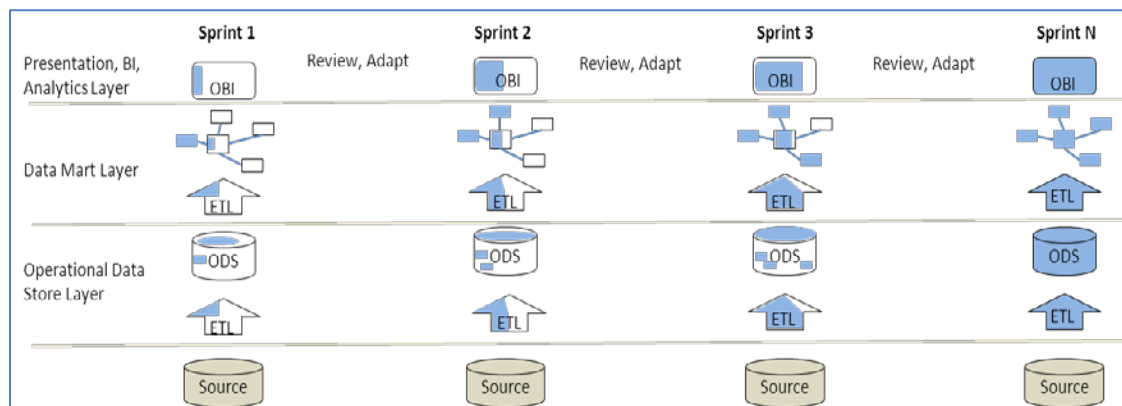
- Liquibase
- GitHub
- ServiceNow
- Jenkins Continuous Integration Server
- JIRA 6.4.1
- Confluence 5.7.3
- Microsoft SharePoint Foundation 2010 (i.e., USCIS Enterprise Collaboration Network (ECN))
- Adobe Connect 9
- ErWin
- Toad
- Microsoft Office suite, to include MS Project and MS Visio

Throughout the execution of this task order, the Government will invest in new tools, technologies, and methodologies that will further enhance DBIS capabilities in meeting its mission. Such transitions and new tools' implementation are within the scope of this task order.

### 3.2. AGILE ANALYTICS APPROACH

USCIS has adopted Agile software development methodology for development of the DW/BI solution, i.e., Agile Analytics approach.

Under the Agile Analytics approach the DW and BI solutions are developed concurrently. Development of the data modeling layer, Operational Data Stores (ODS)/Data Mart layer, Extraction, Transform and Load (ETL) layer, and presentation layer is conducted in several-week sprints to achieve incremental/modular functionality. The following diagram best illustrates the concept:



### 3.3. enterprise CITIZENSHIP & IMMIGRATION SERVICES CENTRALIZED OPERATIONAL REPOSITORY (eCISCOR)

eCISCOR is an operational data warehouse consisting of multiple ODS and several Data Marts. eCISCOR is the sole enterprise data repository and reporting solution for legacy and present day data for the agency. The implementation workload of the enterprise data warehouse will continue to increase as new sources and/or systems are created within the USICS application stack and as more agency forms are migrated to the Electronic Immigration System (ELIS).

eCISCOR presently resides at DHS Data Center 1 (DC1) and has a valid Authority to Operate (ATO). SMART and SAS® are the presentation layers and sub-systems of eCISCOR and have the Authority to Operate under eCISCOR.

eCISCOR consists of three distinct databases:

- PECINTAK – initial staging area for data from all source systems
- PECCON – ODS and Data Repository layer
- PECDW – Data Mart Layer

The intake (PECINTAK) database's sole purpose is data ingestion from source systems of record. Data is stored 'as-is' with limited indexing. Data is then migrated to the Consumer Repository (PECCON), it is mainly migrated 'as-is' or is lightly modified for performance through indexing, partitioning and/or ETL. PECCON is essentially the central point of production for eCISCOR as many internal USCIS applications source this data. Data is further transformed

to the enterprise data warehouse (PECDW) layer for ease of reporting and analytics. The warehouse layer is geared towards comprehensive immigration case tracking where a single petitioner's complete history throughout the benefit process can be followed regardless of the source system for which the case was adjudicated. The warehouse provides for a standardized reporting platform as many systems within USCIS are continuing to transform and modernize. Eventually, the warehouse will become the central point of eCISCOR as the data marts evolve; which will in turn provide a full spectrum of reporting capabilities via conformed dimensions.

The current configuration and architecture of eCISCOR fully supports a centralized data warehouse with increased reliability of connectivity and ingestion of transactional source data. eCISCOR ETLs are also isolated in that data ingestion from the ODS and repository layer is separated from the data warehouse layer. Improvements in High-Availability (HA) have initially been implemented, but further exploration and architecture is needed as the use of eCISCOR has increased dramatically over the past few years. A full Disaster Recovery (DR) solution for eCISCOR is in progress of being established to support the agency's DR requirements. As DBIS further explores the Cloud, the requirement for HA and DR must adapt to the Cloud environment.

There is a substantial increase in need within the agency for the data already stored in the eCISCOR repository. DBIS will continue to standardize the technology around data management and data loading. Working through inconsistent standards for incoming datasets, conversion of Procedural Language/Structured Query Language (PL/SQL) to Informatica ETLs, and setting up data mart structures is an aspect of work that continually needs upkeep.

Informatica PowerCenter (PWC) is the primary ETL tool within eCISCOR - with some residual PL/SQL and Materialized Views within the environment. DBIS is focused on standardizing on a single method of ETL for data ingestion and Dimensional Modeling. Informatica PowerExchange (PWX) is also used in specific applications (such as IDMS Mainframe) and is being implemented for Change Data Capture (CDC) for internal data movement between environments as well as data ingestion from source systems, which users require most current data for reporting purpose.

As a data repository for legacy and current USCIS data, eCISCOR is a connection point and a data hub for various enterprise and legacy applications. This allows for isolating source applications from reporting traffic. eCISCOR expanded its data delivering capabilities by offering initial set of Web Services. Web Services offer common database objects for customers and will allow DBIS the ability to make enhancements that serve the needs of the enterprise customers.

### 3.4. STANDARD MANAGEMENT ANALYSIS REPORTING TOOL (SMART)

SMART is an enterprise-wide BI tool, based on Oracle OBIEE, with close to 3,000 users across USCIS. SMART provides the capability to build and perform self-service analytics and reporting queries on USCIS data to answer business operations and external reporting questions. Currently, SMART is the main presentation layer of eCISCOR and presently includes over 50 topical views of data warehouse data, i.e., subject areas. Subject area structures and naming conventions are based on business requirements to better assist users in the development of their queries. All SMART subject areas are currently managed within one single OBIEE Repository Definition file (RPD). All SMART content, including analysis, agents, actions, and prompts are stored in a single catalog structure. SMART is also directly connected to transactional USCIS systems that require operational reporting that cannot be delayed by an ETL.

SMART is connected to:

- eCISCOR Data Marts - that merge different data sets on the dimensional model structure based on business function. There are currently several marts in production and several under various stages of planning and development
- eCISCOR Operational Data Stores – that are “mirror” copies of the source application systems database. There are currently 20+ ODSes in production, which are available to users for reporting
- Direct Connects – direct connections to the source application transactional database. SMART is connected to 15+ application databases

SMART currently includes several hundred shared catalog folders with thousands of OBIEE catalog items where users create and administer their analysis, dashboards, prompts, and ibots for scheduling reports. Users are divided into three distinct roles:

- Dashboards and Folders Viewers - This role users have access to predefined dashboard reporting areas associated with a specific Subject Areas but cannot edit reports or dashboards
- Dashboard/Folder Administrators - This role allows the user to manage dashboards and reports stored in a specific Subject Area catalog folder
- Subject Area access/Answers Report Developers – This role allows users to build their own ad hoc queries or modify dashboards or reports developed by other users as well as create and distribute scheduled reports

Currently, OBIEE Agents or scheduled reports are used extensively during off peak hours to run queries and have them delivered to the USCIS DHS email addresses. The average size of a SMART query contains 100,000 rows and 5-10 columns; however, some reports require up to 6M of data rows to be included on one report. SMART currently supports on average between 15,000 and 20,000 queries per day.

### 3.5. SAS PREDICTIVE MODELING ENVIRONMENT (SAS PME)

SAS PME supports a growing community of statisticians, economists, operational researchers and analysts who are using SAS for advanced statistical modeling and business intelligence reporting.

The SAS Enterprise BI Server, often referred to as Enterprise Business Intelligence (EBI), was first piloted in 2013. SAS PME has since grown to 200+ users traversing all operational components and headquarters (HQs) offices. Several data repositories are available through SAS, to include:

- eCISCOR ODSes and Data Marts
- Fraud Detection and National Security Data System (FDNS-DS)
- Service Center Computer Linked Application Information Management System (SCCLAIMS)
- External data sets provided by end users

Additional data repositories will become available through SAS as more transactional systems' data become part of eCISCOR and/or connected directly to SAS.

SAS PME supports numerous analytical products developed by users' to better estimate future workload volumes, revenue volumes and temporal immigration trends. Such products are instrumental to USCIS's efficient use of

agency resources. SAS PME supports these functions through thin-client tools and web-based business intelligence applications. These tools allow users to easily access and distribute analyses, reports, and data. For instance, the SAS Information Delivery Portal (SAS Portal) enables users to deliver analytical products, reports and data through an intuitive web-based interface. SAS PME also supports several ETL jobs that clean and integrate data that are pushed into source repositories and used for analytical products and reports.

SAS PME is a tool used for research and analysis where users can extract actionable information from data. Such insight has helped glean answers to questions that are often not possible to determine when using a general reporting tool – e.g., questions such as “why” something happen or “what will happen” in the future.



## 4. TASKS

The contractor shall execute the requirements of this PWS through the following tasks.

### 4.1 TRANSITION-IN

The Contractor shall submit a plan for the Government's approval detailing its planned transition-in activities and address how it will transition with minimal disruption to current operations. The plan shall include a milestone schedule of all transition-in goals, activities, and outcomes. The Government's approval of the plan shall not relieve the Contractor from responsibility for any errors or omissions, nor from responsibility for complying with the requirements of the task order.

The purpose of the transition-in period is for the Contractor to gain familiarity with USCIS OIT processes, procedures, and support activities that will allow it to become fully operational when the transition-in period ends. The transition-in period shall begin 60 days after task order award and shall continue for a period of 60 days.

During the transition-in period, the Contractor shall:

- Provide appropriate staff as defined below who shall be available to work on Day 1 of the transition-in period ensuring transition of knowledge of the DBIS systems and operations from the incumbent Contractor—
  - Development— 12 people (5 each for SMART and eCISCOR and 2 for SAS)
  - Infrastructure— 4 people
  - Program Management – 1person
  - O&M and End User Support – 5 people (at least 1 trainer)
- With such assistance as the Government may provide, perform knowledge transfer of any in-progress documentation, code, and any other materials and artifacts unfinished by the incumbent Contractor
- Obtain full access and operational control over development and test environments to execute system development and testing, as well as appropriate level of access to Stage (System Acceptance Testing Environment) and production environments to execute deployments and system Operations and Maintenance. Obtain access to other auxiliary systems, such as GitHub, JIRA, Jenkins, Liquibase, etc.
- Assume full responsibility for DBIS to include (but not limited to) eCISCOR, SMART, SAS, Informatica operations and support, program management, configuration management, end user training, and service desk support by the end of the Transition In period with minimal interruption to the DBIS operations

### 4.2. SYSTEM DEVELOPMENT

#### 4.2.1 EMERGING TECHNOLOGIES DEVELOPMENT

As USCIS continues to modernize its customer facing and operational lines of business, it relies heavily on aligning these new business models with emerging technologies and IT innovation practices. Implementation of emerging methodologies and technologies shall be expected throughout the implementation of this task order. The

Contractor shall provide technical and program support to research, consult, and implement emerging technologies and practices that the USCIS CIO deems appropriate to support the Agency's goals and objectives.

The following emerging technologies and concepts are currently being implemented within USCIS and shall be supported by the Contractor:

- **Data Visualization:** research, prototype, and implement proprietary and open source data visualization tools to extract information from data in the format useful to senior management and non-technical audiences for decision-making purposes. Provide the capability to identify metrics (KPIs) that can be applied to measure systems and processes' efficiencies and display results in comprehensive, visual format.
- **Microservices :** implementation of service-based architecture within a transactional system that are loosely coupled and replaceable without disturbing other services. Reporting from multiple microservices-based transactional systems will be required.
- **Process and management of big data:** research, prototype, and implementation of tools to process very large data sets in a distributed computing environment (e.g. Apache's Hadoop, no-SQL databases/Graph databases).
- **Advanced Analytical Tools:** research, prototype, and implement statistical programming languages and tools to perform advanced statistical calculations such as parallel algorithms, singular value decomposition, and principal component analysis (e.g. open source R, Python). Research other BI tools that might replace current tools, if they provide better functionality and user experience
- **Cloud:** continue moving all DBIS system components into the Cloud to be set up in the Cloud. Pilot technologies (like RedShift) to enhance analytical capabilities. Set up new proprietary and open source tools in the Cloud to support data exploration, advanced data analytics, and research.

The Contractor shall:

- Research, analyze, and recommend new technology to support the DBIS program mission;
- Support prototyping, testing, and implementation of selected technologies and tools; and
- Provide expert knowledge, technical advice, and data-related consulting services to USCIS.

---

#### 4.2.2 ECISCOR DEVELOPMENT

Data within the data warehouse will be designed in a manner that can allow for relationships and correlations to be readily derived using known facts and attributes such that the data can be fully leveraged for both its known and not yet known business rules. The design of the USCIS DW will follow known data warehousing "best practices" to ensure long-term benefits remain visualized and offset minimal short-term gains.

The centralized data warehouse will be built over time with knowledge obtained through creation of the data marts.

USCIS is developing 10 data marts that are in various stages of completion, to include:

- **Files:** contains the file history and tracks the movement of files
- **Benefits:** contains a collection of all benefits related case management data (e.g. Computer-linked application management system version 3(C3), C4, USCIS Electronic Information System (ELIS, etc.)

- **Scheduling:** contains data for reporting on application interview scheduling (e.g. National Appointment Scheduling System)
- **Customer Service:** designed for storing information from customer interactions (e.g. Service Request Management Tool (SRMT))
- **Fraud/Risk:** contains information needed to track fraud cases and stores additional information needed for fraud detection
- **FOIA:** contains information about documents and tracking of information regarding FOIA requests
- **Verification:** contains information regarding verification status of applicants and customer profile
- **Validation:** contains biometric data components of an applicant
- **Administrative** (Human Resources, Facilities, Financial): contains data from USCIS internal and external transactional systems that execute administrative functions, such as USDA National Finance Center (NFC), hiring systems (both internal and external to USCIS and DHS), facilities management systems, financial systems, etc.
- **Payment:** contains the payment information of a benefit request
- **Person-centric view of the data:** create a person-centric view of the agency data such that an individual full experience with the agency can be traced thru multiple benefits and other tracking and qualifying systems

Additional data marts will be identified as the work on the data warehouse progresses. The priorities for the transactional systems incorporation will be defined by the Government.

The Contractor shall:

- Adopt and comply with the Agile Analytics approach (see § 3.2 above) and provide skills and expertise in Agile development sufficient to apply it effectively to DW/BI development;
- Conduct reviews and assessments of incoming data warehousing requirements to determine both the strategy and development pathway;
- Interact with officially designated product owners, system owners, and business owners of the source systems to understand transactional system data models and elicit requirements and logic for the ETLs;
- Work with the USCIS OIT Government project managers, data architect, transactional system owners, and stakeholders to properly design and architect ODSes and data marts from USCIS major transactional systems. The Contractor shall provide expertise in data modeling and performance optimization. This development will be required to happen concurrently with some transactional source systems' development cycles (such as ELIS);
- Design logical and physical data models that are flexible, expandable, will easily accommodate additions and provide for maintainability. Dimensional models shall be designed to allow for cross-mart reporting;
- Document ODS and data marts design using tools provided by the government (e.g. Erwin);
- Develop one-time ETLs for legacy and or decommissioned data sets to be stored in eCISCOR;
- Document ETL logic in a concise and traceable manner consistent with an Agile development approach;
- Design and develop underlying database(s). Ensure proper design that will allow for optimization, flexibility, and maximum performance. Since multiple ETLs will be performed concurrently, ensure maximum speed of ETL and data ingestion;
- Develop ETL workflows from transactional systems into ODSes and from ODSes into data marts or other type data stores. The design shall ensure minimal impact of ETLs on the transactional systems

performance, implement failure-recovery strategy, and create a load process log that can be used by ETL monitoring and BI tool reporting. The transactional systems are currently based on Oracle, mainframe Integrated Database Management System (IDMS), SQL Server, Pervasive, and Postgres. New database technologies can be utilized by USCIS in the future and the Contractor shall be able to work with these technologies;

- Perform data cleansing and data masking (masking of Personally Identifiable Information (PII) data for development and operational purposes);
- Perform data traceability and maintain the current and accurate mappings;
- Use data enrichment process to enhance data quality from its raw state to the state appropriate for the data warehouse and analytics. Allow for ad-hoc data searches, including wildcard and structured and unstructured data searches;
- Profile and assess data quality and present findings to the Government;
- Execute development utilizing Agile Analytics approach, i.e. utilizing SCRUM Agile development methodology for development of ODSes and data marts;
- Use automated testing tools such as Informatica Data Validation Option (DVO) for database regression testing and testing against changing source systems' schemas;
- Maintain automated database deployments via Liquibase;
- Deploy finished code to production environment in accordance with scheduled deployments (as frequently as required);
- Re-develop existing ETL code written in PL/SQL and MViews into Informatica workflows;
- Demonstrate and provide expertise, knowledge, and skill in major tools used for development (Oracle, Informatica, SAS) as well as knowledge and expertise in applying Agile development to DW and tools associated with Agile development execution (such as JIRA);
- Interact with OIT support organizations to comply with existing OIT processes, such as Quality Assurance, Configuration Management, engineering support groups, etc.;
- Advise the government on the best approach to achieve optimization and maximum performance in ETL executions, database performance, and physical architecture of the data warehouse;
- Execute other activities related to development work, such as participate in meetings, provide briefings, presentations and other support materials that will promote the program, assist in achieving user buy-in, and explain technical concepts to non-technical audiences;

The Contractor shall possess a proficient level of knowledge of Informatica, which includes developing and implementation with the following Informatica modules:

- Test Data Management;
- Identity Resolution Option;
- Address Doctor;
- Change Data Capture;
- Data Quality;
- Data Validation; and
- PowerExchange for IDMS mainframe systems.

The above Informatica modules are currently owned by the Government; additional modules of the Informatica tool may be procured, which will be utilized and implemented by the Contractor.

---

#### 4.2.3 BI DEVELOPMENT

Under this task the Contractor shall provide services to plan, design, develop, implement, and test new BI functionality to support new reporting capabilities based on customer business requirements. Subject area design, structure, and presentation shall follow best practices and provide an “easy to use and understand” user experience. This task shall also include development of reports/queries for specific business requirements, data discrepancy analysis and resolution, and validation of report output against source systems or other data sets. The product owners will be prioritizing the requirements that can come from the SMEs and/or business users.

The Contractor shall:

- Adopt and comply with the Agile Analytics approach (see § 3.2 above) and provide skills and expertise in Agile development sufficient to apply it effectively to DW/BI development;
- Participate in requirements discussions and analysis with USCIS business users and designated Product Owners to understand reporting business needs, supporting business processes, associated USCIS form types or work products, consumers of data for analysis or reports;
- Plan and size application level development work in preparation for Agile sprint development;
- Produce user stories for Agile sprints based on specific user business requirements and maintain healthy backlogs in JIRA;
- Develop all application code needed to fulfill user stories;
- Execute unit, integration, functional testing as well as adjustments from user acceptance testing of code and functionality using non automated and automated methods during all Agile sprint cycles;
- Develop operational and analytical reports, and/or dashboards to meet specific customer requirements for the particular work stream activity;
- Follow presentational and developmental guidelines for naming conventions and report functionality to provide a consistent, standardized, and efficient end user experience;
- Develop reporting capabilities, which effectively handle large database queries and complex logical SQL scripts. Maintain accurate representation of work completed and Work-In-Progress (WIP) in JIRA;

---

#### 4.2.4 SAS DEVELOPMENT

The Contractor shall be responsible for helping to create content for USCIS users as USCIS offices continue to train their employees on how to effectively use the SAS tool. Contractor staff shall assist users in all facets of content development ranging from accessing data through SAS Add-In for Microsoft Office, creating reports and data in SAS Web Reports Studio to developing algorithms to support the agency in making data-driven decisions. If needed, the Contractor shall assist in small to medium size development projects; however, the primary focus of SAS development will be to enable users to integrate the tool into their local operations.

The Contractor shall:

- Migrate and/or re-create SAS content that was developed using desktop SAS software modules. (Note: SAS PME is an enterprise server-based solution and users throughout USCIS may still be using local instances of SAS. As the enterprise instance gains wider acceptance, content migration and re-creation will become an important aspect of SAS development);
- Assist users with the development of analyses, reports, dashboards, stored procedures, portal pages, information maps, ETLs, SAS cubes, data quality reports, and advanced analytical models using various SAS modules;
- Analyze disparate data requirements and help users to develop automated solutions for USCIS workflows and processes; and
- Provide quality deliverable(s) for all SAS development solutions that will be free of syntactical and logical errors in code and mathematical expression and will run error free in all environments

---

#### 4.2.5 TESTING AND EVALUATION SUPPORT

The Contractor shall follow all USCIS Agile testing methodologies, DHS or USCIS Software Enterprise Lifecycle (SELC) (Agile track) processes as well as any government, DHS or USCIS compliance guidance or mandates.

The Contractor shall:

- Execute and adhere to Dev/Ops and Agile non-automated and automated testing techniques, tools and practices to ensure fully tested software;
- Execute Section 508 testing and adhere to Section 508 Standards for all electronic and information technology products interacting with end-users;
- Demonstrate Agile sprint user stories' developed functionality to appropriate business participants for user acceptance testing; and
- Remediate any security related testing defects in either deployed software or in the technology stack.

---

#### 4.2.6 CONFIGURATION MANAGEMENT AND SYSTEM SECURITY POSTURE

A change is an addition, modification or removal of approved, supported or baseline hardware, network, software, application, system, image or associated documentation. USCIS follows an Agile based software development process, which aligns with a Change, Configuration and Release Management (CCRM) environment. The Contractor shall provide support for completion of all activities related to the USCIS CCRM with the Agile application release processes and software releases shall be managed in the software release tool (i.e., GitHub Enterprise).

The Contractor shall:

- Create Staging and Production Change Requests in the Change Management tool (i.e.,ServiceNow);
- Prepare all necessary documentation and participate in semi-annual (or more frequent) Release Planning Reviews (RPRs);
- Maintain all technical and security documentation for all releases in USCIS electronic document library ITDL and USCIS ECN (SharePoint) including (e.g. Product Backlog, Training Plan, and test scripts);
- Maintain code baseline in code repository (GitHub Enterprise);
- Develop and maintain Pipeline Design Documentation;

- Manage all Agile sprint user stories, backlog in electronic management tool (i.e., Jira);
- Develop and maintain documentation including Plan of Action and Milestones POA&Ms, Section 508 Compliance Determination and Remediation Form, Systems' Privacy Threshold Assessments (PTAs), Privacy Impact Assessments (PIAs), System Security Plans;
- Maintain current active Authority to Operate and adhere to Security procedures to maintain ongoing authorization; and
- "Re-ATO" the system in the public Cloud, once moved. Work with USCIS Information Security Division (ISD) to implement new security procedures in the Cloud environment and ensure that DBIS is in full compliance with Information and Cyber Security requirements.

#### 4.3. OPERATIONS AND MAINTENANCE (O&M)

The Contractor shall provide full O&M support of the operational DBIS systems' components.

##### 4.3.1. O&M - ECISCOR

Under this task, the Contractor shall conduct initial incident, problem and change management resolution in addition to being responsible for the overall monitoring, tuning, adjustments, and health of the eCISCOR data warehouse, corresponding transformational scripts, interoperability, backups, and connectivity.

The Contractor shall:

- Actively monitor the Oracle Automatic Workload Repository (AWR) for operational database(s) system performance on a daily basis and provide database tuning, monitor database growth, monitor daily logs, manage database logs
- Work closely with USCIS Enterprise Infrastructure Division (EID) DBAs, System and Network Administrators to ensure routing and remedy of system and network performance issues;
- Provide databases administration in coordination with government technical staff, DBIS Infrastructure Team, and EID DBAs;
- Ensure data flows through all eCISCOR database environments properly (i.e., PECINTAK to PECCON, PECCON to PECDW, PreProd, DR);
- Assist the user community and application interfaces in writing well-performing SQL code;
- Administer operating system and database functions that are not fully supported by EID, notably any operations within the Cloud (Monitor performance degradations and ongoing maintenance involving OS, FTP Servers, Network, Database, Job Scheduler) ;
- Monitor system usage, report utilization, and proper system access in accordance with the developed security model and provide statistics to USCIS federal staff;
- Spot trends in queries and create and maintain summary tables for low-performing queries where possible;
- Support the execution of emergency backups in coordination with other infrastructure operational components and/or DHS data center specific requirements ;
- Verify database are routinely backed up and that Oracle Recovery Manager (RMAN) is operating properly throughout the database environments; and
- Coordinate outages and scheduled downtime.

ETL:

- Provide resolution to Incident (failures/missing or invalid data, delayed data), problem (repeated incidences not permanently fixed) & change management (bug/break fixes; enhancements)
- Enhance ETL based on source system changes or evolving new requirements including implementation of minor system changes involving the Informatica PowerCenter and PowerExchange application
- Troubleshoot and fix ETL related bugs reported by end-users

---

#### 4.3.2. O&M - SMART

The Contractor shall be responsible for SMART presentation layer enhancements to existing DBIS products including Direct Connect SMART Subject areas, Marts, Operational Data Stores, and mainframe sources. O&M activities shall include OBIEE RPD fixes, report authoring per user story requirements and, mainframe Database Management System (DBMS) changes managed via Kanban O&M releases.

The Contractor shall:

- Document requirements (user stories) and conduct analysis for SMART subject area adjustments;
- Design, develop and test SMART reports and dashboards based on customer user stories;
- Maintain, manage, and update the O&M backlog in JIRA;
- Manage multiple simultaneous customer requirements into Kanban sprint cycles based on Government assigned priority;
- Facilitate and manage customer requirements and development status meetings and reviews;
- Deploy finished code to production based on the Kanban schedule when the code is ready for production deployment;
- Respond to emergency break-fix situations to correct obvious mistakes and inaccurate data presentation;
- Conduct data traceability at customer request to validate and prove data accuracy;
- Interact with multiple field customers, answer their questions, and conduct all communication in the professional manner; and
- Warn customers of planned and emergency system outages via group-mail communication.

---

#### 4.3.3 O&M - SAS

Continued administration, monitoring, tuning and development of the SAS environment is essential to ensuring SAS users are provided with an optimal system capable of meeting USCIS's demand for analytics.

The Contractor shall:

- Administer SAS PME instance(s) covering all facets of the SAS enclave – to include but not limited to: user account management, system group management, system role management, general system access,



system content review, system debugging and troubleshooting, filesystem security and configuration, system monitoring, SAS services monitoring, system security and general system patching;

- Assist users with SAS module functionality, to include enabling users to develop and maintain any/all analytical products, content and reports;
- Provide expert and quality customer service to all SAS PME users;
- Ensure all licensed SAS software and services are configured and available for use by SAS PME users;
- Assist with testing and optimizing SAS code, jobs and analyses to ensure efficient use of system resources;
- Maintain, manage, and update the SAS Kanban board in JIRA;
- Provide uninterrupted service with the operational system to the end users; and
- Ensure that all system outages will have a persistent solution to prevent continued system problems.

#### 4.4. END USER SUPPORT AND CHANGE MANAGEMENT

##### 4.4.1. SYSTEMS ISSUE INTAKE

The Contractor shall be responsible for the intake, issue tracking management, administration and timely resolution support of end user issues or questions related to eCISCOR and its data sets, SMART and SAS PME operational functionality, or other DBIS related topics or product lines.

The Contractor shall:

- Manage and administer the USCIS ServiceNow SMART and SAS PME Groups which includes customer issues and questions;
- Manage and administer MS Outlook SMART and SAS PME mailboxes which are the primary conduit for intake of customer issues and questions;
- Maintain Tier II and III tickets in Jira and manage and track resolution;
- Develop and maintain ServiceNow Knowledge Management Scripts for SMART, eCISCOR, and SAS PME;
- Develop and maintain SMART/eCISCOR/SAS PME internal Standard Operating Procedures with regards to intake and communication management processes; and
- Conduct timely resolution of SMART and SAS incident tickets-
  - Tier II –ticket resolution within 5 business days;
  - Tier III - ticket resolution within 10 business days from Tier II receive date.

##### 4.4.2. TRAINING DEVELOPMENT AND DELIVERY

The Contractor shall provide user-appropriate and targeted training activities of the DBIS suite of tools. Training can be done on production data and serve as the ultimate data quality validation by the user community. The Government will review training content prior to Contractor execution.

Training shall be targeted to the users' level of familiarity (beginner, intermediate, advanced) with the tool, reports, and data. Users who are new to the systems shall first be trained on the tool, then on the data and reports. Users, who are familiar with the tool, shall be trained on new data sources and their structure, ad-hoc models, and new canned reports.

Training shall facilitate change management, specifically, it shall promote system applicability to users' day-to-day activities, and how it facilitates and complements their job related duties, and demonstrates business value.

Trainers shall be familiar with OBIEE and SAS tools (and any other BI tool implemented throughout execution of the task order) functionality and well-versed in specific data marts' structures and data models. Business users shall be provided examples that they can relate to and be able to learn how to use the tool effectively on the job. Training development shall follow the Agile Analytics approach and be developed as the work on specific system features and data sets are being completed.

In addition, the Contractor shall provide supporting documentation to ensure users who have been trained on the system can have material to refer to (such as PowerPoint slides, data dictionaries, data model diagrams), which is aimed at reinforcement of knowledge required to use the system effectively.

The Contractor shall:

- Support the business community with knowledge, skills, and abilities to utilize SMART (and any other BI tool implemented throughout execution of the task order) effectively on their jobs;
- Develop and maintain a SMART standard training catalog at a minimum to include—
  - SMART beginner training module with introductions to use of dashboards,
  - Report author training including the use of filters,
  - Report layout including the use of pivots and other presentational methods, and
  - SMART catalog and dashboard management and administration modules;
- Provide training modules that will include PowerPoint content, live system demonstrations and hands on practical exercises;
- Develop and maintain SMART Custom Subject Area training as new marts or updated data sets become available to users;
- Deliver training catalog or custom training offerings to be delivered in both: classroom (at Government locations) and webinars formats;
- Develop and maintain eCISCOR data workshops for either existing eCISCOR data sets, new eCISCOR data sets, or SMART direct-connects for both: classroom and webinars (e.g. C3 Consolidated, Benefits Mart, iCLAIMS);
- Manage and administer ECN (SharePoint site) electronic training calendar;
- Provide SMART functional systems training and data workshops to support meeting new and existing end users operational mission duties;
- Create one new data workshop every other month; and
- Deliver one data workshop a month.

The Contractor shall also be responsible for providing SAS specific training covering all licensed SAS modules and any future SAS modules the Government plans to procure (the Government can modify and/or expand the SAS training outline listed below at any time). Training material will cover module specific functionality as well as descriptive and predictive statistical analysis interpretation.

The Contractor shall:

- Provide SAS users and managers with the knowledge, skills and ability to use and implement SAS reporting and analysis module(s) within the local office(s); and
- Develop a standard training program<sup>2</sup> for beginner, intermediate and advanced SAS Enterprise Guide (EG) users that includes—
  - Standard data integration techniques for merging external data sources with SAS Libraries and imported datasets ;
  - Querying techniques using SAS syntax and the graphical user interface (GUI) query builder;
  - Performing descriptive and predictive statistical analysis;
  - Creating standard/shared reports and analysis and distribute via Microsoft and via the SAS web applications;
  - Simple SAS syntax techniques (including data steps structure and proc structure), and
  - Performing statistical analysis using the SAS EG GUI.

USCIS currently has close to 3000 SMART and 250 SAS PME users who perform a variety of activities with these tools including the development of interactive reports and dashboards, analytical forecasting and trend analysis, management and administration of scheduled reports for executive and operational needs across all of the eCISCOR and Direct Connect data sets. As the user base grows with first time users, existing users become more sophisticated as well as with the addition of new marts and data sets into eCISCOR a robust end user support capability needs to be in place to address users' issues and questions and build USCIS Program capacity with regards to reporting and analytics knowledge.

In order for USCIS to adopt the eCISCOR data sets and SMART reporting and analytic tool as part of its business operations, the Contractor shall be responsible for a wide range of change management products and activities.

The Contractor shall:

- Develop and maintain subject area data dictionaries;
- Develop and maintain task level job aids for SMART functionality;
- Maintain and administer SMART ECN to contain tools, resources and information for SMART users;
- Develop follow-up of annual SMART/eCISCOR customer survey;
- Develop and deliver episodic and monthly end user SMART group mail communications;
- Facilitate and support of Integrated Project Teams which will address topics such as new or updated subject areas/data sets, reporting requirements resulting from the migration of form types to different systems, and data validation issues;
- Develop a quarterly SMART electronic newsletter; and
- Use the SMART/SAS/eCISCOR resources, products, tools and information to empower end users with better knowledge of reporting and analytical capabilities.

#### 4.5 INFRASTRUCTURE SUPPORT

---

<sup>2</sup> USCIS, as a customer of SAS, is eligible to utilize SAS standard training provided by the SAS institute. Contractor-developed training can utilize SAS materials that should be adapted to USCIS-specific usage of SAS and its functionality.

The Contractor shall assume Infrastructure support for the database, ETL, BI layer, SAS, and OS, if applicable (in the Cloud), as well as the developed systems components of DBIS.

---

#### 4.5.1 ECISCOR DATABASE INFRASTRUCTURE SUPPORT

Under this task the Contractor shall support all tools including maintenance (upgrade, patching, etc.) and performance tuning along with the following:

- Cooperate with government technical staff in providing O&M support of the production components of eCISCOR, SAS PME, and SMART. Provide technical assistance to either the onsite IT personnel or IT deployment support personnel to resolve failures, and support incident management and problem management activities;
- Support all tools and infrastructure upgrades and their set up in the Cloud;
- Support DBIS O&M with coordination of appropriate DHS/USCIS Data Center support staff and USCIS OIT Engineering Support to diagnose, trouble shoot and resolve system, network, hardware and software issues;
- Provide technical expertise and support the DevOps software lifecycle/development methodology;
- Support DBIS Development teams with Automated deployments technology such as continuous integration, continuous deployment (CI/CD);
- Enhance system performance thru partitioning, multi-threading, etc. to achieve maximum infrastructure utilization;
- Troubleshooting data discrepancy and missing data issues including ETL load failures due to resource constraints, missing/invalid data/files, bugs and infrastructure component issues;
- Evaluate performance degradations and ongoing maintenance involving ETL toolset, OS, File Transfer Protocol (FTP) Servers, Network, Database, Job Scheduler;
- Set up the governors and event triggers on the database systems to stop runaway queries;
- Monitor, diagnose, and troubleshoot and resolve, as needed, under-performing OBIEE SMART queries;
- Execute software upgrades of all environments (development, stage, pre-production, production) for SMART, SAS PME, and eCISCOR, as upgrades are determined to be required;
- Assist with the preparation and support the development of contingency plans and assist with conducting plan tests, including disaster recovery and Continuity of Operations Plan (COOP) testing, and operation failover testing consisting of documented contingency plans. The Contractor may be required to develop and/or provide input to contingency plans for USCIS IT applications. The Contractor may be required to assist responsible DHS and USCIS parties in planning and executing Disaster Recovery (DR) for SMART, SAS PME, and eCISCOR system components;
- Maintain Personal Identity Verification (PIV) system authentication as directed by USCIS; and
- Support migrations to new infrastructure (the Cloud).

---

#### 4.5.2 ETL ADMINISTRATION

The Contractor shall:

- Be responsible for administration of the Informatica layer;

- Troubleshoot data discrepancy and missing data issues resulting from daily ETL loads;
- Monitor ETL load failures due to resource constraints, missing/invalid data/files, bugs and infrastructure component issues;
- Monitor performance degradations and ongoing maintenance involving ETL toolset;
- Monitor ETL completions and logs and provide status of data loading including Database Management Systems (DBMS) Jobs, which entail data intake. Perform ETL failure recovery when needed. Daily notifications on ETL completions will be required to ensure no interruption in service; and
- Monitor file-based data sources loading according to the established schedule.

---

#### 4.5.3 SAS ADMINISTRATION

The Contractor shall:

- Monitor the full architecture of the SAS environment to ensure optimal configuration and performance;
- Diagnose infrastructure and performance problems and recommend and implement optimal solution;
- Provide expert solution options for SAS architecture configuration(s);
- Support the installation/re-installation and configuration of SAS environments – test, stage, production and/or Cloud environment;
- Assist USCIS OIT Engineering in system patching and upgrades that are provided by the SAS Institute;
- Develop server-side scripts to help automate administrative tasks (using Solaris, Linux and/or Windows OS); and
- Administer operating system and SAS application that are not fully supported by EID, notably any operations within AWS or any other USCIS Cloud solution.

---

#### 4.5.4 OBIEE ADMINISTRATION

The Contractor shall:

- Maintain and manage SMART Direct Connections to Oracle, SQL Server, and Postgres databases;
- Maintain and administer OBIEE catalog structure, permissions, items and groups;
- Administer application for security configuration settings to configure row-level security access to data and Single Sign On (SSO);
- Monitor and administer performance and availability including performance tuning;
- Manage code consistency across all environments (e.g. test, stage, pre-production, production);
- Manage and administer backup and recovery procedures for application layer;
- Manage and administer scheduled and unscheduled outages and down time;
- Manage and administer automated deployments;

- Ensure continuity between primary and disaster recovery sites. DR must always be operationally ready to be activated; and
- Maintain a Recovery Time Objective (RTO) of 24 hours from the point of Disaster Recovery Activation.

#### 4.6 PROGRAM MANAGEMENT

The Contractor shall provide Program Management support for planning, execution, and completion of all project activities in accordance with DHS and USCIS Agile procedures. While USCIS will provide management 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 to this task who will manage the day-to-day activities of the Contractor staff.

The Contractor Project Manager shall be an employee of the Prime Contractor and have responsibility for the accomplishment of the task order. The Project Manager shall organize, direct, and coordinate the planning and execution of all activities, review the work of subordinates, including subcontractors, and ensure that the schedule, performance parameters, and reporting responsibilities are met. The Project Manager shall integrate the Contractor's management and technical activities across this Task Order to ensure they are consistent.

The Contractor's Project Manager shall be the primary interface with the USCIS Program Manager or designee. Attendance at weekly status meetings and ad hoc meetings is required.

All lead personnel on the Task Order shall possess not only management skills, but technical skills as well and be hands-on executors, rather than just managers.

Project Management shall ensure that Contractor staff organize and participate in all activities associated with Agile development methodology, to include, but not limited to, daily stand up meetings, sprint planning, sprint review, and sprint retrospective meetings. Independently of the number and size of subcontractors the prime Contractor partners with, the Contractor shall present a united team to the Government.

The Contractor will be required to form and maintain more than one Agile development team and shall be able to manage multiple Kanban/SCRUM/Agile Analytics engagements (such as, pursue development on several data marts simultaneously). The Contractor shall maintain healthy, well-managed user story backlog for every work stream in JIRA, to include backlog grooming with respective Product Owners and the overall capacity planning with the Government DBIS Program Manager, who is also the DBIS overall Product Owner.

At the request of the COR, the Government Program Manager, or a Government Project Manager, the Contractor shall be required to prepare briefing materials, deliver briefings, participate in meetings with USCIS organizations and/or external organizations, and present program content. The Contractor shall develop, as necessary, written recommendations, oral presentations and/or executive briefing materials.

The following meetings are mandatory for the Contractor to attend and will be scheduled by the Government:

- Task Order Kick-Off meeting
- Technical Kick-Off meeting

- Weekly status meeting with Government staff. The Contractor PM and technical leads shall participate in person at the location designated by the Government
- Monthly Program Management Review meeting. The Contractor PM and technical leads shall participate in person at the location designated by the Government
- Other ad-hoc meetings scheduled by USCIS senior leadership or Government team

In accordance with best program management practices, the Contractor shall:

- Maintain proper **cost** control, submit accurate invoices and financial Internal Use Software (IUS) reports, request approval of overtime premiums under cost-reimbursement CLINs via the COR and the Program Manager, and provide cost clarifications at the Government's request;
- Maintain a Program Roadmap that denotes **schedule** commitments, timely report to the Government on variation and changes to the Roadmap, and provide schedule information at Government request, such as planned activities for the next 90 days, and anticipated deployments;
- Provide information on compliance with the contract **performance** parameters in the format agreed-upon with the Government during monthly Program Management Review meetings. Self-report performance issues; and
- Maintain a **Risk** Registry in the format agreed-upon with the Government (JIRA preferred) and report major risks during monthly Program Management Review meetings. Suggest risk mitigation strategies and execute them upon Government agreement.

The Contractor shall be responsible for submitting a Quality Control Plan (QCP) within 30 days after Technical Kick-Off meeting that provides details of how the Contractor will ensure the quality of deliverables and standard of performance on the Task Order. The Contractor shall provide accomplishments and performance highlights at the weekly status meetings and formally during the Program Management Review (PMR) meeting. The Contractor shall disclose to the government any performance concerns within the Contractor's team and take appropriate actions to improve performance prior to Government involvement.

The Contractor will be required to interact with multiple other contractor teams. The Government expects full Contractor cooperation, proper meeting attendance, and good faith efforts to accomplish joint work.

#### 4.7 TRANSITION-OUT

The Contractor shall execute the transition-out activities on a month-to-month basis, (not to exceed 90 days) from the time of the new task order award notification by the Government. The Contractor shall execute the transition-out in good faith and with minimal disruption to current or future Government operations.

Deliverables include:

- Transition-Out Plan; and
- Transition-Out activities, as defined in the Transition-Out plan.

The Contractor shall prepare a Transition-Out plan within 15 days from receiving the aforementioned notification from the Government. The Transition-Out Plan shall include, but not limited to, identification of all products (documentation, code, and other artifacts) in progress that need to be transitioned, Government Furnished Equipment (GFE), software in use that was furnished by the Government, and access permissions to all

environments and systems. The Government will provide specific instructions for transition execution as they will apply to the situation.

## 5. TASK ORDER ADMINISTRATION

### 5.1. DELIVERABLES

The Contractor shall submit the deliverables that are indicated in the table below to the Government COR, Program Manager (PM), and Contracting Officer (CO). The Contractor shall inquire about the Government's required format for all deliverables prior to commencing any effort on the tasking. The Contractor will be notified in writing by the COR upon final acceptance of all deliverables. In addition to the deliverable requirements indicated in the table, each USCIS IT Application shall have deliverable requirements associated with the respective Section 4 Task Descriptions. The Project Manager shall include, as part of each Monthly Status Report, Monthly PMR, and Ad Hoc Reporting, those specific deliverable requirements that are based on the indicated deliverables, and in addition, tailored to the applicable provisions of USCIS SELC/Agile policies and/or USCIS CCRM.

The Contractor shall provide all necessary personnel and deliverables based on the required delivery date(s) established by mutual agreement between the Government and the Contractor in the Task Order. Administrative deliverables consist of revised and/or updated Task Order Plans, Progress Reports, Financial Reports, and Performance Reports. Progress and Financial reports shall be prepared and distributed in accordance with the Task Order. The Task Order monthly IUS report shall include cost information reported at the subtask level, as discussed in Attachment II. The Progress Reports and Financial Reports shall be submitted in a mutually agreeable manner – for the reported elements and the report format - to the USCIS Project Manager and servicing agency for each of the projects tasks/systems. An electronic copy in a mutually agreeable file format shall accompany the hard copies of the progress and financial reports.

Deliverables required by the SELC / Agile methodologies for a given phase are determined by the phase of the project and the work pattern specified in the proposal incorporated into the PWS upon award of the Task Order. The Contractor shall provide an electronic copy of the task schedule information in Microsoft (MS) Project to facilitate the coordination of this task with other Government and Contractor activities, so that the schedule information can be disseminated to USCIS field offices. The Government will use a central repository to jointly maintain the schedule.

Upon receipt of the Government comments, the Contractor shall, within 5 business days, rectify the situation and re-submit the Task Order deliverable(s) if it is not a "draft" deliverable. If it is a "draft" deliverable, the Contractor shall rectify the situation before the next scheduled submission of this deliverable.

### 5.2. SCHEDULE OF DELIVERABLES

The table below aggregates all the deliverables that are part of this Task Order:

Deliverables
--------------



Reference	Requirement	Description	Due Dates
Section 4.1	Transition-in Schedule and Plan	Schedule and Plan to complete all transition-in activities within 60 days	15-days after Technical Kick-off meeting
Section 4.2	Code	System code promoted to production via automated CI/CD with GitHub Enterprise as a focal point	In accordance with scheduled sprint deployments
Section 4.2.4	SELC (Agile track) system documentation	Submitted to USCIS electronic library	In accordance with scheduled sprint deployments
Section 4.2.5	Security Authorization Package (to include Privacy documentation) in accordance with DHS requirements, FISMA, and NIST standards	Security Authorization package, updates to Security Authorization documentation, POA&M remediation activities, and Privacy required documentation	According to FISMA schedule and on-going security activities
Section 4.4.2	Training materials User training manual Course Catalog	Appropriate system training materials customized to the audience	Per the schedule developed during execution
Section 4.4.3	Change management products	Subject area data dictionary, task level job aids, and SMART newsletters	As required
Section 4.6	Program Roadmap	In a format agreed upon by government and contractor	Continuously maintained jointly with the Government PM, updated at a minimum each sprint
Section 4.6	Quality Control Plan	Quality Control Plan detailing Contactor quality control procedure	30-days after the Technical Kick-off meeting

Deliverables			
Reference	Requirement	Description	Due Dates
Section 4.6	Risk Registry	Risk Registry in the format agreed upon during execution	Continuously maintained jointly with the Government PM, updated at a minimum on a weekly basis
Section 4.6	Weekly Status Meeting	Review of current activities, ongoing work requirements, and problems/issues.	Weekly Status Meeting is to be coordinated through the Government PM for time/day to remain consistent with agency requirements
Section 4.6	Program Management Review (PMR)	PMR concise accurate project information in the form of a “quad chart” in the form of MS PowerPoint slides	30 days into Task Order performance and monthly thereafter. PMR date and time will be scheduled by the Government on a monthly basis. The PMR slides are due the day before scheduled PMR meeting
Section 4.6	Monthly Status Report	Monthly Status Report (Two separate sections consisting of Technical Performance and Business Performance)	Monthly after transition begins (to be submitted at the same time as PMR and delivered to the COR and ITPgM).
Section 4.6	Briefings/Documents	Documents and briefings outside of normal weekly meetings. Requests issued by the COR or the Government PM	As required
Section 4.6	Task Order Kick-off Meeting (Post Award Conference)	Business focused conference aimed at describing the overall scope of Task Order work	Within 11 business days after Task Order award

Deliverables			
Reference	Requirement	Description	Due Dates
Section 4.6	Technical Kick-off Meeting	Follow on meeting with/between the Contactor and Federal technical teams that is technical in nature	Within 15 business days after Task Order award
Section 4.6	Financial Report (to include IUS Report)	<p>Overview financial report (part of PMR) and IUS report:</p> <ul style="list-style-type: none"> <li>Hours and Cost (segregated into two areas - development and deployment)</li> <li>This data is to be reported separately from the invoice.</li> </ul>	30 days into Task Order performance and monthly thereafter. To be delivered NLT 10 business days after month's end. Financial information in the PMR should be delivered per PMR delivery schedule
Section 5.9	Telework Plan	Contractor's Corporate Telework Plan	1 business day prior to the Task Order-Award Kickoff Meeting
	Separation Notification	The CO and COR must be notified of each contract employee termination/resignation.	Within five (5) days of each occurrence
	Redacted Copy of the order to Freedom of Information Act (FOIA)	Submit a redacted copy of the executed order to FOIA by email at <a href="mailto:foiaerr.nrc@uscis.dhs.gov">foiaerr.nrc@uscis.dhs.gov</a>	Within 30 days of award

### 5.3. PLACE OF PERFORMANCE

The principal place of performance shall be at a Contractor provided work site. The off-site Contractor facility shall be within reasonable travel distance (not to exceed 20 miles) of 111 Massachusetts Ave NW, Washington D.C. 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.

To facilitate efficient collaboration with product owners, business SMEs, and systems users the contractor is expected to require of some of its team members (such as Business Analysts and SCRUM Masters) that they commute to the government facility at 111 Massachusetts Ave NW, Washington D.C. 1-2 days a week. The Government has limited space, but can provide hoteling space for 4-5 people on a daily basis.

#### 5.4. KEY PERSONNEL

The following personnel are considered key personnel and shall possess the following skills, level of experience, and certifications:

Labor Category	Role on the Program	Required Certification(s)
Project Manager	Provide overall authority and responsibility for the Contractor Task Order management and execution (1 CFTE). Must be employed by the Prime.	<p>Program Management Professional (PMP) and Information Technology Infrastructure Library (ITIL) certifications</p> <p>At least 5 years of professional experience managing large data warehouse projects</p> <p>Knowledge of and ability to organize the team to perform Agile Analytics development proven by professional experience</p>
Solutions Architect (Senior) – Development Technical Lead	Provide expert team leadership and guidance on development efforts. Lead overall system architecture and design (1 CFTE)	<p>Bachelor of Science degree in Computer Science, Engineering or related subject and at least 5 years of experience leading architectural design of a large data warehouse.</p> <p>Knowledge of and ability to organize technical execution of Agile Analytics proven by professional experience</p> <p>Certification in one of the following: Oracle, Informatica, or Amazon Web Services</p>
Systems Engineer (Senior) – Infrastructure Lead	Provide expert technical leadership to manage, monitor, and ensure the highest level of availability of all operational systems and infrastructure within DBIS (1 CFTE)	<p>Bachelor of Science degree in Computer Science, Engineering or a related subject and at least 5 years of experience maintaining and administering infrastructure of IT systems comparable to DBIS.</p> <p>Certification in one of the following: Oracle, Informatica, or Amazon Web Services</p>

Labor Category	Role on the Program	Required Certification(s)
Business Intelligence (Systems Engineer)	Provide technical expertise and team direction for the implementation of BI functionality (1 CFTE)	At least 5 years of experience developing and implementing BI solutions.  Certification: Oracle Business Intelligence Foundation Suite 11g (or 12c) Essentials or other industry-accredited BI tool
Functional Analyst (Senior)	Lead analyst for overall business and systems requirements to ensure end user product satisfaction (1 CFTE)	At least 5 years of experience leading Business Analysis effort on a large IT system implementation
Lead Trainer	Lead training content development and all training efforts.	At least 3 years of experience overseeing training programs and developing complex technical training content.  Familiarity with OBIEE required
SAS Solutions Architect (Systems Engineer)	Lead SAS Solutions Architect with experience administering an enterprise SAS solution with users exceeding 200. (1 CFTE)	At least 5 years of direct experience administering, developing and implementing SAS solutions. Certification in one of the following: SAS Certified Platform Administrator for SAS 9 SAS Certified Advanced Programmer for SAS 9 SAS Certified BI Content Developer for SAS 9

Labor Category	Role on the Program	Required Certification(s)
Subject Matter Expert III  (all staff designated as a SME III)	Provide expert guidance on Data Warehousing and Business Intelligence systems and associated tools. Provides expert technical leadership to project team(s)	<p>At least 10 years of experience in the technical subject in which the individual is designated as SME proven by professional experience and certifications.</p> <p>Certification in <u>one</u> of the following:</p> <ul style="list-style-type: none"> <li>• Oracle Database 11g or higher Administrator Certified Professional</li> <li>• Oracle Database 11g or higher Administrator Certified Master</li> <li>• Informatica Certified Professional,</li> <li>• Informatica PowerCenter Administrator - Expert or Master</li> <li>• Informatica PowerCenter Data Integration Certification</li> <li>• Informatica Data Quality and Data Governance Enterprise edition</li> <li>• Informatica Master Data Management Certification</li> <li>• AWS Certified Solutions Architect – Professional</li> <li>• AWS Certified DevOps Engineer</li> <li>• AWS Certified SysOps Administrator</li> <li>• Certified Jenkins Engineer</li> </ul>

The Contractor shall ensure the project is staffed with an adequate number of assigned personnel possessing the required certifications, qualifications, skills and experience with the Business Intelligence technologies as described above.

The Contractor shall identify key personnel, provide a statement of qualifications and resume for each of these individual upon task award and at any time a substitution is proposed. The statement of qualification will include a YES or NO declaration for meeting each of the requirements and the resume will show how the individual meet the requirements for the position.

## 5.5 GOVERNMENT-DIRECTED TRAVEL

Travel outside of the Metropolitan Washington, DC area to USCIS service centers and field offices will be required for some staff. In the event travel is required, travel shall not be performed in connection with this Task Order without prior approval in writing (email for the request and approval is acceptable) by the COR. The Contractor shall be reimbursed for travel in accordance with para. (d) of the EAGLE II parent contract clause B.4.1.2, Time and Material (T&M) Task Orders. Upon completion of travel, all documentation associated with the respective travel shall be submitted with the invoices in the next billing cycle. Reimbursement for local travel is not authorized.

Local travel is defined as official travel necessary to conduct business within a 50-mile radius of the Government facilities.

## 5.6 GOVERNMENT FURNISHED PROPERTY

The Government will furnish the following property to the Contractor staff upon successful Enter-on-Duty (EOD):

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	\$1,800	TBD	TBD	TBD	TBD
PIV card	After EOD	Upon departure	EA	\$500	TBD	-	TBD	TBD

The Government will not be obligated to provide additional accessories for the laptop computers, such as monitors, computer bags, external mice, etc. 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.

## 5.7 GOVERNMENT FURNISHED INFORMATION

The Government will provide licensing for the following Software to be used by the Contractor. If the Government decides to procure additional software to be used by DBIS, the Government will provide the licensing for that software.

Software	Date/Event Indicate when the SW will be furnished	Date/Event Indicate when the SW will be returned
Informatica (current version used by the Government)	Upon EOD the Contractor will be able to load the software on the GFE computer	Upon departure with return of GFE
Oracle Database and OBIEE (current version used by the Government)	Upon EOD the Contractor will be able to load the software on the GFE computer	Upon departure with return of GFE

<b>Software</b>	<b>Date/Event Indicate when the SW will be furnished</b>	<b>Date/Event Indicate when the SW will be returned</b>
SAS (current version used by the Government)	Upon EOD the Contractor will be able to load the software on the GFE computer	Upon departure with return of GFE
Quest TOAD for Oracle (current version used by the Government) up to 5 licenses	Upon EOD the Contractor will be able to load the software on the GFE computer	Upon departure with return of GFE
Erwin Data Modeler (current version used by the Government) up to 8 licenses	Upon EOD the Contractor will be able to load the software on the GFE computer	Upon departure with return of GFE
JIRA (current version used by the Government)	Upon EOD the Contractor will be able to load the software on the GFE computer	Upon departure with return of GFE
MS Project and MS Visio based on duties on the project, up to 5 licenses	Upon EOD the Contractor will be able to load the software on the GFE computer	Upon departure with return of GFE

At a minimum, the Government will provide the Contractor access to the following informational resources and support systems:

<b>Informational Resource/ Systems</b>	<b>Date/Event Indicate when the SW will be furnished</b>	<b>Date/Event Indicate when the SW will be returned</b>
System access – contractor staff will be provided access to all DBIS systems’ dev-test-stage-pre-prod-prod environments. Access will be provided to staff based on job duties	Upon authorized EOD and full BI adjudication (required for access to Prod environment)	Access will be terminated upon contractor departure
DHS, USCIS intranet and email system	Upon EOD	Access will be terminated upon contractor departure
Access to support systems (JIRA, GitHub, ServiceNow, etc.)	Upon EOD	Access will be terminated upon contractor departure



The Contractor will be exposed to additional informational resources while working with USCIS, such as DHS and USCIS policies and management directives, informational meetings, demonstrations by other programs and vendors, business SOPs, etc.

## 5.8 HOURS OF OPERATION

Normal duty hours will be between 7:00 am to 7:00 pm, Monday through Friday, excluding Federal Government Holidays. Contractors shall be available during this time period. On occasion, the Contractor may need to adjust this schedule to accommodate emergencies, outside of business hours system deployment, and maintenance activities, or high priority deadlines. Contractors shall not be permitted to work more than 40 hours per week, excluding holidays, unless advance written permission has been granted by the COR.

## 5.9 TELEWORK

Contractor may authorize its employees to telework in support of this task order after the review and acceptance of the Contractor's Corporate Telework Plan by the contracting officer. The Contractor's Corporate Telework Plan is due one (1) business day prior to the Task Order Kick-off Meeting. Before beginning to telework, all employees shall complete the annual Computer Security Awareness Training (CSAT) requirement, access to which shall be provided by USCIS. The Contractor shall report monthly to the COR the number of employees teleworking, the number of hours teleworked, productivity, other data requested by the CO, and any issues related to teleworking.

Telework shall be considered a privilege, not a right, and shall not impact Contractor's productivity and participation in any Agile sessions or government meetings.

The Government reserves the right to restrict Contractor employees' telework, if the Government determines that it impacts proper execution of the requirements of this task order.

**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 31<sup>st</sup> 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](mailto: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.



### **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*.

## **COMPUTER AND TELECOMMUNICATIONS SECURITY REQUIREMENTS**

### **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](mailto: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.

## **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 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 30<sup>th</sup>. 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 30<sup>th</sup> 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.