AWARD/CONTRACT	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE OF PAGES 1 46

2. CONTRACT (Proc. Inst. Ident.) NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUEST/PROJECT NO.
70SBUR18C00000017	See Block 20C	OPQ180014

5. ISSUED BY	CODE	6. ADMINISTERED BY (If other than Item 5)	CODE
USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403	CIS		

7. NAME AND ADDRESS OF CONTRACTOR (No., street, country, State and ZIP Code)	8. DELIVERY	9. DISCOUNT FOR PROMPT PAYMENT
VERTICAL APPLICATIONS INC 42694 MIDDLE RIDGE PLACE BROADLANDS VA 201485512	☐ FOB ORIGIN ☒ OTHER (See below)	Net 30
	10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN	ITEM
CODE 9627777230000	FACILITY CODE	

11. SHIP TO/MARK FOR	CODE	12. PAYMENT WILL BE MADE BY	CODE
Office of Performance & Quality 111 Massachusetts Ave NW Suite 3000 Washington DC 20529	OPQ	See Invoicing Instructions	WEBVIEW

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:	14. ACCOUNTING AND APPROPRIATION DATA
☐ 10 U.S.C. 2304 (c) ( ) ☒ 41 U.S.C. 3304 (a) (5)	See Schedule

15A. ITEM NO	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	Continued				
	15G. TOTAL AMOUNT OF CONTRACT				

16. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
X	A	SOLICITATION/CONTRACT FORM	1-2	X	I	CONTRACT CLAUSES	18-26
	B	SUPPLIES OR SERVICES AND PRICES/COSTS				PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
X	C	DESCRIPTION/SPECS./WORK STATEMENT	3-14	X	J	LIST OF ATTACHMENTS	27-46
	D	PACKAGING AND MARKING				PART IV - REPRESENTATIONS AND INSTRUCTIONS	
	E	INSPECTION AND ACCEPTANCE			K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
	F	DELIVERIES OR PERFORMANCE					
	G	CONTRACT ADMINISTRATION DATA			L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
X	H	SPECIAL CONTRACT REQUIREMENTS	15-17		M	EVALUATION FACTORS FOR AWARD	

CONTRACTING OFFICER WILL COMPLETE ITEM 17 (SEALED-BID OR NEGOTIATED PROCUREMENT) OR 18 (SEALED-BID PROCUREMENT) AS APPLICABLE

17. ☒ CONTRACTOR'S NEGOTIATED AGREEMENT (*Contractor is required to sign this document and return* 1 *copies to issuing office.*) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. *(Attachments are listed herein.)*

18. ☐ SEALED-BID AWARD (*Contractor is not required to sign this document.*) Your bid on Solicitation Number 70SBUR18R00000070 including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your bid, and (b) this award/contract. No further contractual document is necessary. (Block 18 should be checked only when awarding a sealed-bid contract.)

19A. NAME AND TITLE OF SIGNER (Type or print)	20A. NAME OF CONTRACTING OFFICER
[redacted]	TRACEY B. HARRIOT
19B. BY [redacted] (Signature of person authorized to sign)	19C. DATE SIGNED 9/25/2018
20B. UNITED STATES OF AMERICA BY (Signature of the Contracting Officer)	20C. DATE SIGNED 26SEP2018

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition is NOT usable

STANDARD FORM 26 (Rev. 3/2013)
Prescribed by GSA - FAR (48 CFR) 53.214(a)

NAME OF OFFEROR OR CONTRACTOR

VERTICAL APPLICATIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	DUNS Number: 962777723+0000 This firm-fixed price contract for Data Strategy Development Support Services is awarded in accordance with the Section 8(a) Partnership Agreement between the Small Business Administration and the Department of Homeland Security. AAP Number: APFS #2018043632 FOB: Destination Period of Performance: 09/26/2018 to 09/25/2019				
0001	Data Strategy Development Support Services in accordance with the attached Statement of Work FFP Accounting Info: CDOSTRG 000 EX 50-01-00-000 23-90-0000-00-00-00-00 GE-25-14-00 000000 Funded: Accounting Info: CDOSTRG 000 EX 20-01-00-000 23-90-0000-00-00-00-00 GE-25-14-00 000000 Funded:	12	MO		
1001	Data Strategy Development Support Services in accordance with Statement of Work FFP Amount: (Option Line Item) 08/25/2019 Accounting Info: Funded: The total amount of award: The obligation for this award is shown in box 15G.	7	MO		

US CITIZENSHIP AND IMMIGRATION SERVICES

Statement of Work

Office of the Chief Data Officer

Chief Data Officer Data Strategy

September 2018

CONTENTS

Statement of Work

Chief Data Officer Strategy

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 administers the nation's lawful immigration, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the Homeland, and honoring our values.

To execute its mission USCIS has over 19,000 Government employees and Contractors working at 250 offices worldwide. One of USCIS' main strategic objectives is continuous improvement of its operations and migration to the electronic intake and adjudication of the immigration benefits – the eProcessing initiative.

1.2. CDO MISSION

USCIS is the largest custodian of lawful immigration data in the Federal Government. Not only does it depend on data to adjudicate applications, but as a fee based agency, it is dependent on these data to project revenue and make staffing decisions. As its data assets continue to grow at a fast pace and the agency is faced with the need to advance to a paperless processing environment, USCIS must focus on developing a solid enterprise data strategy. Strategic data management will ensure that the agency acquires, ingests, generates, maintains, manages, stores, and shares data in the most efficient and mission-focused manner.

The Office of the Chief Data Officer (CDO) resides within the USCIS Management Directorate, Office of Performance and Quality (OPQ). It was recently established to improve the agency data posture and to tackle the issues that have been known and observed by the USCIS business operations, as well as IT programs.

The mission of the USCIS CDO is to ensure that the agency makes timely, high-quality data available to internal and external stakeholders to fulfill the mission of the agency. In that capacity, the CDO office is aligned with the OPQ mission of providing relevant, accurate, and data-driven analyses enabling USCIS to make effective, data-driven decisions.

2. OBJECTIVE AND SCOPE

2.1. OBJECTIVE

The objective of this requirement is to obtain professional services for the USCIS CDO to conduct the initial assessment of the USCIS data assets, identify and properly document data issues facing the agency, and assist the CDO in developing the data strategy to improve the USCIS data posture.

In meeting these objectives, the Contractor will be expected to collaborate with multiple business stakeholders to conduct the work; specifically, with the Office of Information Technology (OIT), Service Center Operations Directorate (SCOPS), Field Office Directorate (FOD), and other USCIS business stakeholders. Furthermore, the contractor will be expected to interact with DHS governance bodies and structures when it pertains to development of the DHS data posture and USCIS' input into these activities.

The contractor will be exposed to multiple USCIS IT programs and business initiatives and will be expected to cooperate and interact with multiple contractor groups. The government expects seamless cooperation and productive interaction among all involved parties.

2.2. SCOPE

The contractor shall be responsible for providing professional support services for the CDO to meet the objectives of conducting the initial assessment of the USCIS data assets, identifying and properly documenting data issues facing the agency, and assisting the CDO in developing the data strategy to improve the USCIS data posture as outlined throughout this document.

3. CURRENT STATE

3.1. OFFICE OF PERFORMANCE AND QUALITY

OPQ is the source of USCIS immigration and operational production statistics. USCIS Leadership requires precise data-driven analysis and insight derived from immigration and operational data in order to develop the policies and procedures to guide the operations of the Agency directorates, program offices, and serve the Front Office. OPQ fulfills this need by creating an environment that fosters teamwork in order to deliver the highest level of customer service that will provide accurate, high quality, data-driven analyses, enabling our stakeholders to make effective business decisions in a timely manner.

The majority of the OPQ functions and products focus on:

- Supporting the agency's ability to measure how long it takes USCIS to process cases;
- Forecasting the volume of receipts for all USCIS form types and other workloads;
- Developing staffing allocation models for most USCIS offices and directorates;
- Providing statistical modeling around USCIS' ability to reduce the current backlog of cases;
- Developing monthly, quarterly, and annual National Performance Reports;

- Providing support to the Office of the Chief Financial Officer to assess currently in-place fees and development of the future fee structure to ensure the agency is properly compensated for its work;
- Satisfying the majority of the agency data-based FOIA requests;
- Providing reporting for external partners and stakeholders; and
- Publishing data sets on the USCIS' publicly facing websites for public consumption, such as academia, researchers, and other interested parties

In this capacity, OPQ works with all agency data gathered via multiple IT systems and utilizes reporting and statistical tools available via OIT. Specifically, OPQ statisticians work with the SAS tool (SAS Predictive Modeling system) to conduct statistical modeling, forecasting, and predictive analysis. OPQ utilizes the Standard Management Analytics & Reporting Tool (SMART), which is based on Oracle OBIEE as a report generation tool, and it uses traditional tools like MS Excel and MS Access to pull and analyze various data sets.

3.2. OFFICE OF THE CHIEF DATA OFFICER

The Office of the Chief Data Officer is a new office within OPQ that was stood up in July 2018. It is responsible for the agency enterprise data governance, data standards formulation and adoption by all IT programs, as well as development of standard reporting products that are consumed by the operations and senior management. Furthermore, the CDO will be responsible for formulating and implementing the agency data strategy and will assume responsibility and product ownership for the agency data warehouse and ad-hoc reporting platforms and tools.

4. TASKS

The contractor shall execute the requirements of this SOW through the specific tasks described below. At a high-level the tasks include:

- Baseline assessment of the USCIS enterprise data assets:
    - Assessment of the current data quality from multiple core transactional systems
    - Assessment of the core business data (intake data) and adjudications data from essential case management systems and major transactional systems
    - Assessment of the reference data compliance
    - Assessment of the systems' data being generated by the transactional systems in support of the adjudication process and downstream reporting needs
    - Development of metrics and benchmark criteria to conduct the above assessments
- Formulation of the best communications channels to ensure compliance with developed data standards and data governance practices
- Assisting the CDO in formulating the portfolio of initiatives based on the assessment that will allow the CDO to formulate the agency data strategy and the implementation roadmap
    - Documentation of the data strategy and the roadmap based on CDO guidance

4.1 BASELINE DATA ASSESSMENT

The contractor shall develop the initial methodology and conduct the essential inventory and assessment of the USCIS data assets. The contractor shall be responsible for identifying the benchmark criteria, the assessment methodology, and documenting the results of the assessment.

USCIS has a number of IT systems that collect, generate, and process core agency business data. For example, USCIS has five case processing systems – Computer Linked Application Management System 3 (CLAIMS 3), CLAIMS 4, Electronic Immigration System (ELIS), Global (not an acronym; a case management system for asylum applications), and Investor File Adjudication Case Tracker (INFACT). Some of these systems are legacy (like C3 and C4) and some are very new and are still being developed (ELIS, Global, and INFACT).

As part of this task, the contractor shall assess the data gathered at intake, and generated as part of the adjudications process, to determine the data standards that are being adopted by these systems, and their compliance with the developed data standards. The outcome of this assessment will be a comprehensive view that indicates how uniformly (or not) these systems intake data and how much of the core business data is being collected (since some systems' data is being keyed-in manually from the paper form submissions (C3 and C4) and others (ELIS) intake the immigration form data electronically). Furthermore, a similar assessment will be conducted for the systems' compliance with the developed reference data, as well as how well the databases of these systems are equipped with audit columns that allow the downstream reporting systems and the data warehouse to get meaningful data for reporting purposes.

Similar assessments will be done for other types of systems – records tracking, scheduling, customer service, etc. There are approximately 30 different IT systems in the enterprise that contribute to the overall processing of the immigration benefits and represent core business systems.

Data quality assessment is another area where the contractor shall dedicate significant efforts. USCIS has used electronic systems for various parts of the business process for a number of years. As the technology and the business practices continuously evolve, OIT has been modernizing legacy, developing new, and decommissioning old and outdated business systems. Data quality from legacy systems as well as from the newly developed systems is of concern as the current data quality does not allow USCIS to merge data easily and report from it on the overall workload of case processing. USCIS has challenges implementing programmatic ways of sharing data between the systems and "stitching" data together in the data warehouse because data management is currently treated as part of an individual IT program or system.

The contractor shall advise the CDO on the best path forward in terms of data quality as it relates to the legacy data.

4.2. DATA GOVERNANCE AND COMMUNICATONS

The contractor shall formulate the best path forward for developing and proliferating the data standards. The Contractor shall work with the CDO to improve the communication channels with the IT programs so that the standards get properly utilized during the IT development cycles.

The contractor shall advise the CDO on the best practices of implementing a robust governance structure to circulate information and solicit sound business decisions from the data stewards and the Subject Matter Experts. The contractor shall assist with revamping the existing governance structure.

The contractor shall develop and establish the communications plan/strategy on how data should be incorporated into the OIT portfolio of IT projects and how to achieve the ultimate state of quality data and solid data structures/architecture that can be "developed once and used multiple times" by systems and end-users.

4.3. DATA STRATEGY AND ROADMAP DEVELOPMENT

The contractor shall apply all the knowledge gathered from the data assessment and the governance and data standards development to assist the CDO in formulating the data strategy for the agency.

The strategy shall outline the roadmap from the defined current state to the desired state and accentuate the difference. The strategy shall focus on the benefits to USCIS of the data strategy implementation and identify how it will support the business vision. The strategy shall also include anticipated change management challenges and mitigation strategies.

4.4. PROGRAM MANAGEMENT

The contractor shall provide program management support for planning, execution, and completion of all project activities in accordance with best project management practices. The contractor shall assign a project manager who shall be responsible for all work performed under this contract. The program manager is designated as Key Personnel as outlined in section 5.3.4 below.

At the request of the COR, or the government program 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:

- Post-Award Conference
- Technical Kick-Off meeting
- Weekly status meeting with Government staff. The contractor PM and technical staff shall participate in person at the location designated by the Government
- Other ad-hoc meetings scheduled by USCIS senior leadership or Government team

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.

5. CONTRACT ADMINISTRATION

5.1. DELIVERABLES

The contractor shall submit the deliverables that are indicated in the table below to the Government COR, and program manager at a minimum. Additional recipients may be identified throughout contract performance on a case-by-case basis.

The format for deliverables will be pre-approved by the government. The contractor will be notified in writing by the COR upon final acceptance of all deliverables. The government will provide written acceptance, comments, or change requests, if any, within 10 business days of receipt. If acceptance, comment, or change requests are not received within 10 days, this shall represent acceptance unless notified otherwise. Upon receipt of government comments, the contractor shall make necessary revisions within five business days and resubmit if it is not a

"draft" deliverable. If it is a "draft" deliverable, the contractor shall make necessary revisions before the next scheduled submission of the deliverable.

5.2. SCHEDULE OF DELIVERABLES

The following technical deliverables are required under performance of this contract. Additional contractual deliverables shall be submitted in accordance with the applicable clause, term, or condition.

Deliverables			
Requirement	**Requirement**	**Description**	**Due Dates**
Section 4.1	Baseline Data Assessment	Format mutually agreed upon	3 months after the technical kick-off meeting
Section 4.1	Data Quality Assessment	Format mutually agreed upon	6 months after the technical kick-off meeting
Section 4.2	Communications Strategy	Format mutually agreed upon	6 months after the technical kick-off meeting
Section 4.3	Data Strategy and Implementation Roadmap	Format mutually agreed upon	Initial strategy - 6 months after the technical kick-off meeting Iteration of the strategy – every 3 months thereafter for the duration of the POP

5.3. PLACE OF PERFORMANCE

The principal place of performance shall be 111 Massachusetts Ave NW, Washington D.C. Meetings will generally 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.

5.4. KEY PERSONNEL

The government shall have the opportunity to review the qualifications, education and experience of proposed key personnel to ensure compliance with this section. In accordance with HSAR 3052.215-70, before removing or replacing key personnel, the contractor shall submit sufficient information to support the proposed action to the contracting officer at least 10 days before the effective date of the proposed change.

5.4.1 PROJECT MANAGER

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 be the single point of contact for the contracting officer and contracting officer's representative (COR) and primary interface with the USCIS program manager. The project manager shall be employed by the prime contractor.

The project manager shall have Project Management Professional (PMP) certification and at least five years of experience in comparable positions.

5.4.2 SOLUTION ARCHITECT (SENIOR)

The solution architect shall provide expert team leadership and guidance in performance under this contract. It is expected that this key personnel position shall be responsible for leading the overall data assessment and strategy development efforts.

The solution architect shall have a Bachelor of Science in Computer Science, Engineering, or related subject and at least five years of experience leading architectural design.

5.5 GOVERNMENT FURNISHED PROPERTY

The Government will furnish the following property to the contractor staff upon successful Entry-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)	Manufacturer & Model Number	"As-is"
Laptop computer with power cord and desk lock	After EOD	Upon departure	EA	$1,800	TBD	TBD	TBD	TBD

5.6 GOVERNMENT FURNISHED INFORMATION

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

Informational Resource/ Systems	Date/Event Indicate when the SW will be furnished	Date/Event Indicate when the SW will be returned
System access – contractor staff will be provided access to USCIS systems. 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

Informational Resource/ Systems	Date/Event Indicate when the SW will be furnished	Date/Event Indicate when the SW will be returned
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.

5.7 HOURS OF OPERATION

Normal duty hours will be between 7:00 am to 6:00 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.

5.8 TELEWORK

Contractor employees may be authorized to telework in support of this contract after the review and acceptance of the contractor's telework plan by the contracting officer. The contractor's telework plan is due 15 days after the post-award conference.

The Government reserves the right to restrict contractor telework if the Government determines that it negatively impacts proper execution of the requirements.

5.9 ITAR LANGUAGE

Accessibility Requirements (SECTION 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All deliverables provided as electronic documents shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. Applicable standards include:
   - All WCAG Level A and AA Success Criteria Apply
   - All support services and document requirements

2. When developing or modifying electronic documents that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at https://www.dhs.gov/compliance-test-processes.

3. When providing deliverable upgrades, substitutions, or replacements to electronic document deliverables, the contractor shall not reduce the original electronic document's level of Section 508 conformance before the upgrade, substitution or replacement.

4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards

5. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

6. Where electronic documents conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the electronic documents that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

DHS Security Policy Requirement

The following terms and conditions will be included in all acquisition documents.

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

Encryption Compliance Requirement

The following terms and conditions should be included in all acquisition documents.

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.

2. National Security Agency (NSA) Type 2 or Type 1 encryption.

3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

Security Review

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

SECTION H – Special Contract Requirements

Section 8(a) Partnership Agreement

This contract is entered into between the U.S. Small Business Administration (SBA) (Prime contractor) and the 8(a) Participant (subcontractor) and the Department of Homeland Security (DHS), U.S. Citizenship & Immigration Services (USCIS).

The 8(a) Partnership Agreement (PA), dated 10/23/2012, issued between the SBA and DHS delegates the authority to make direct award of the contract to the 8(a) participant once the requirement has been offered and accepted by the SBA. The DHS USCIS Contracting Officer will retain contract administration.

ADDITIONAL INVOICING INSTRUCTIONS:

INVOICE SUBMISSION INSTRUCTIONS (Addendum to FAR 52.212-4(g))
(a) Each invoice shall contain the following information:
(1) Contract No.
(2) Name of the Contract Specialist or Contracting Officer
(b) Each invoice must be submitted to the designated billing office via one of the following modes (listed in descending order of preference):
(c) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.
(d) 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 using the "To" line in the e-mail address to **USCISInvoice.Consolidation@ice.dhs.gov** with each email conforming to a size limit of 500 KB.
(e) If a paper invoice is submitted, mail the invoice to:

USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

Special invoicing instructions for unfilled labor categories/positions: In the event that any labor category/position remains unfilled for 30 business days or more, the Contractor shall multiply the unfilled labor rates(s) by eight (hours) for each day the labor category/position remains absent starting on the 31st day; the Contractor shall then subtract that amount from the total invoice amount for each month the labor category/location remains unfilled.

PERFORMANCE REPORTING

The Government intends to record and maintain contractor performance information for this contract in accordance with DHS FAR Class Deviation 11-03. The contractor shall enroll at www.cpars.gov for participation in this process.

NOTICE TO PROCEED (NTP)

Full contract performance shall commence on the date specified by the Contracting Officer in the Notice to Proceed directive.

(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 complete packages from contractor employees in order to receive favorable entry-on-duty (EOD) decisions and suitability determinations. 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 contract.

(c) The Contractor shall submit background investigation packages immediately following contract award.

(d) This contract 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 for performance to begin no later than 30 days after contract award. The contracting officer will issue a notice to proceed at least one day before performance is to begin. If the Government decides to issue the NTP prior to all contractor employees being able to perform, there will be a reduction of price based upon the proportion of contractor employee's available to begin work.

POSTING OF CONTRACT (OR ORDER) IN FOIA READING ROOM

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

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

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

FAR 52.222-54, Employment Eligibility Verification

In accordance with this clause, the contractor is required to enroll as a Federal Contractor in the E-Verify program within 30 calendar days of contract award. Once enrolled, the contractor is required to use E-Verify to electronically verify employment authorization of: (1) all new employees hired during the contract term; and (2) all employees performing work in the United States on the contract. Some exemptions may apply, please see guidance at www.uscis.gov/e-verify/federal-contractors on who is to be verified.

The contractor shall provide assertion of its enrollment in E-Verify and use of the system within 30 days of contract award to the Contracting Officer to include any applicable employee exemptions. If these assertions are not received or it cannot be completed, the contractor shall provide a plan to ensure compliance with the clause. The assertion shall be from the prime contractor and each subcontractor.

SECTION I – Contract Clauses

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses: http://www.acquisition.gov/far.

(End of clause)

FAR Clauses Incorporated By Reference

52.203-17, CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (APR 2014)

52.204-9 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011)

52.212-4 CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (JAN 2017)

52.223-10 WASTE REDUCTION PROGRAM (MAY 2011)

52.245-1 GOVERNMENT PROPERTY (JAN 2017)

FAR Clauses In Full Text

52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (JAN 2018)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)

(3) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(4) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

_X_ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

_X_ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

___ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).

_X_ (4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Oct 2016) (Pub. L. 109-282) (31 U.S.C. 6101 note).

___ (5) [Reserved]

_X_ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

___ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

_X_ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Oct 2015) (31 U.S.C. 6101 note).

_X_ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

___ (10) [Reserved]

___ (11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).

___ (ii) Alternate I (Nov 2011) of 52.219-3.

___ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

___ (ii) Alternate I (Jan 2011) of 52.219-4.

___ (13) [Reserved]

_X_ (14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).

___ (ii) Alternate I (Nov 2011).

___ (iii) Alternate II (Nov 2011).

___ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

___ (ii) Alternate I (Oct 1995) of 52.219-7.

___ (iii) Alternate II (Mar 2004) of 52.219-7.

_X_ (16) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)).

___ (17) (i) 52.219-9, Small Business Subcontracting Plan (Jan 2017) (15 U.S.C. 637 (d)(4)).

___ (ii) Alternate I (Nov 2016) of 52.219-9.

___ (iii) Alternate II (Nov 2016) of 52.219-9.

___ (iv) Alternate III (Nov 2016) of 52.219-9.

___ (v) Alternate IV (Nov 2016) of 52.219-9.

_X_ (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).

_X_ (19) 52.219-14, Limitations on Subcontracting (Jan 2017) (15 U.S.C. 637(a)(14)).

___ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

___ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).

_X_ (22) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).

___ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).

___ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).

_X_ (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

_X_ (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2018) (E.O. 13126).

_X_ (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

_X_ (28) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

_X_ (29) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

_X_ (30) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

_X_ (31) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

_X_ (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

_X_ (33) (i) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

___ (ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).

_X_ (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

___ (35) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

___ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

___ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).

___ (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).

___ (38) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514

___ (ii) Alternate I (Oct 2015) of 52.223-13.

___ (39) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).

___ (ii) Alternate I (Jun 2014) of 52.223-14.

___ (40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

___ (41) (i) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).

___ (ii) Alternate I (Jun 2014) of 52.223-16.

_X_ (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011) (E.O. 13513).

___ (43) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).

___ (44) 52.223-21, Foams (Jun 2016) (E.O. 13696).

_X_ (45) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

_X_ (ii) Alternate I (Jan 2017) of 52.224-3.

___ (46) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).

___ (47) (i) 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

___ (ii) Alternate I (May 2014) of 52.225-3.

___ (iii) Alternate II (May 2014) of 52.225-3.

___ (iv) Alternate III (May 2014) of 52.225-3.

___ (48) 52.225-5, Trade Agreements (Oct 2016) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

_X_ (49) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

___ (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

___ (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

___ (52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

___ (53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505), 10 U.S.C. 2307(f)).

___ (54) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

_X_ (55) 52.232-33, Payment by Electronic Funds Transfer— System for Award Management (Jul 2013) (31 U.S.C. 3332).

___ (56) 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).

___ (57) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

_X_ (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

_X_ (59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(12)).

___ (60) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

___ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

[*Contracting Officer check as appropriate*.]

___ (1) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495)

___ (2) 52.222-41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67.).

___ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

___ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (May 2014) (29 U.S.C.206 and 41 U.S.C. chapter 67).

___ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

___ (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).

___ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

___ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E.O. 13658).

___ (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

___ (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).

___ (11) 52.237-11, Accepting and Dispensing of $1 Coin (Sep 2008) (31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iv) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.

(v) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vi) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

(vii) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(viii) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(ix) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

(x) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xi) 52.222-41, Service Contract Labor Standards (May 2014), (41 U.S.C. chapter 67).

(xii) (A) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(xiii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)

(xiv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)

(xv) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xvi) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(xvii) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xviii) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xix) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xx) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxi) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within **15 days**; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **30 days**. 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 **19 months**.

(End of Clause)

HSAR CLAUSES IN FULL TEXT:

HSAR 3052.212-70 CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

(b) Clauses.

X 3052.204-71 Contractor Employee Access.

X Alternate I

X 3052.205-70 Advertisement, Publicizing Awards, and Releases.

X 3052.215-70 Key Personnel or Facilities

Project Manager

Solution Architect (Senior)

X 3052.242-72 Contracting Officer's Technical Representative.

(End of clause)

SECTION J – List of Attachments

Attachment	Title
1	Security Requirements, 8 pages
2	Safeguarding of Sensitive Information, 9 pages
3	Information Technology Security and Privacy Training, 2 pages

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 DHS Form 11000-25, Contractor Fitness/Security Screening Request Form and the USCIS Continuation Page to the DHS Form 11000-25. 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 DHS Form 11000-25 and the USCIS Continuation Page to the DHS Form 11000-25 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. DHS Form 11000-25 "Contractor Fitness/Security Screening Request Form"

5. USCIS Continuation Page to DHS Form 11000-25

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

7. Foreign National Relatives or Associates Statement

EMPLOYMENT ELIGIBILITY

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

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

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

CONTINUED ELIGIBILITY

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

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

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

December 31st each year, or prior to any accelerated deadlines designated by USCIS, 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 Insider Threat Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure Training** (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **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, Version 10*, May 2016
- 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:
https://etms.uscis.dhs.gov/ContentDetails.aspx?id=32609AFDFA97494CA3319DCE12FC1B43
or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

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

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

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

SECURITY ASSURANCES

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

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

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*.

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Definitions.* As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: 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), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, 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 Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of

the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

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

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

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their 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 is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in

these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA

in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting

Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements*.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training

is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)