

2. CONTRACT (Proc. Inst. Ident.) NO. 70SBUR18C00000013	3. EFFECTIVE DATE See Block 20C	4. REQUISITION/PURCHASE REQUEST/PROJECT NO. OIT186026 / OIT186042
---	------------------------------------	--

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

7. NAME AND ADDRESS OF CONTRACTOR (No., street, country, State and ZIP Code) SIMPLE TECHNOLOGY SOLUTIONS INC 1775 I STREET NW SUITE 1150 WASHINGTON DC 20006	8. DELIVERY <input type="checkbox"/> FOB ORIGIN <input checked="" type="checkbox"/> OTHER (See below)
	9. DISCOUNT FOR PROMPT PAYMENT Net 30
	10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN ITEM

CODE 0791971690000	FACILITY CODE
--------------------	---------------

11. SHIP TO/MARK FOR CODE HQOIT Department of Homeland Security US Citizenship & Immigration Svcs Office of Information Technology 111 Massachusetts Ave, NW Suite 5000 Washington DC 20529	12. PAYMENT WILL BE MADE BY CODE WEBVIEW See Invoicing Instructions
---	--

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C. 2304 (c) () <input checked="" type="checkbox"/> 41 U.S.C. 3304 (a) ()	14. ACCOUNTING AND APPROPRIATION DATA See Schedule
---	---

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

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	1-3	X	I	CONTRACT CLAUSES	25-49
	B	SUPPLIES OR SERVICES AND PRICES/COSTS		PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
X	C	DESCRIPTION/SPECS./WORK STATEMENT	4-21	X	J	LIST OF ATTACHMENTS	50
	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			L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
	G	CONTRACT ADMINISTRATION DATA			M	EVALUATION FACTORS FOR AWARD	
X	H	SPECIAL CONTRACT REQUIREMENTS	22-24				

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

17. <input checked="" type="checkbox"/> CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return <u>1</u> 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. <input type="checkbox"/> SEALED-BID AWARD (Contractor is not required to sign this document.) Your bid on Solicitation Number _____ 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) XXXX XXXX	20A. NAME OF CONTRACTING OFFICER XXXX XXXX
--	---

19B. NAME OF CONTRACTOR BY _____	19C. DATE SIGNED 7/23/2018 9:13 AM EDT	20B. UNITED STATES OF AMERICA	20C. DATE SIGNED 7/23/18
---	---	-------------------------------	---------------------------------

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
70SBUR18C00000013

PAGE OF
2 50

NAME OF OFFEROR OR CONTRACTOR
SIMPLE TECHNOLOGY SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	<p>DUNS Number: 079197169+0000 This contract for the development of an Innovation Lab for the USCIS Office of Information Technology (OIT) is awarded in accordance with the Section 8(a) Partnership Agreement between the Small Business Administration and the Department of Homeland Security. SBA Reference No. 0353/18/0468 AAP Number: 2018041813 FOB: Destination Period of Performance: 07/23/2018 to 10/22/2020</p> <p>Base Period 07/23/2018 - 10/22/2018</p> <p>Development of an Innovation Lab through the use of a Digital Minimally Viable Product (MVP) in accordance with (IAW) the Statement of Work (SOW). This is a XXXX CLIN.</p> <p>Accounting Info: ITBNATZ C30 EX 20-01-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Funded: \$XXXX</p> <p>Accounting Info: ITBNATZ 000 EP 20-05-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Funded: \$XXXX</p>	3	MO	XXXX	XXXX
0002	<p>Travel - Not to Exceed (NTE) \$XXXX. Obligated Amount: \$XXXX</p> <p>Accounting Info: ITBNATZ 000 EP 20-05-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Funded: \$XXXX</p> <p>Option Period One 10/23/2018 - 10/22/2019</p>	1	LO	XXXX	XXXX
1001	<p>Development of an Innovation Lab through the use of a Digital MVP IAW the SOW. This is a XXXX CLIN. Amount: \$XXXX (Option Line Item) 10/01/2018</p> <p>Accounting Info: Funded: \$XXXX</p>	12	MO	XXXX	XXXX
1002	<p>Travel - NTE \$XXXX. Continued ...</p>	1	LO	XXXX	XXXX

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
70SBUR18C00000013

PAGE OF
3 50

NAME OF OFFEROR OR CONTRACTOR
SIMPLE TECHNOLOGY SOLUTIONS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
2001	<p>Amount: \$XXXX (Option Line Item) 10/01/2018</p> <p>Accounting Info: Funded: \$XXXX</p> <p>Option Period Two 10/23/2019 - 10/22/2020</p> <p>Development of an Innovation Lab through the use of a Digital MVP IAW the SOW. This is a XXXX CLIN.</p> <p>Amount: \$XXXX (Option Line Item) 10/01/2019</p> <p>Accounting Info: Funded: \$XXXX</p>	12	MO	XXXX	XXXX
2002	<p>Travel - NTE \$XXXX.</p> <p>Amount: \$XXXX (Option Line Item) 10/01/2019</p> <p>Accounting Info: Funded: \$XXXX</p> <p>CONTRACT ADMINISTRATION: The contractor shall not accept any instruction that would result in any change to the supplies or services herein by any entity other than the issuing office's Contracting Officer (CO). The following is delegated to the Contract Specialist (CS) and Contracting Officer's Representative (COR). COR is responsible for technical monitoring, receiving and accepting the product or service and verifying the invoicing of one time purchase of firm fixed price supplies. The CS is a procurement official who assists the CO in all aspects of the contracting functions. The CS will review and approve proper, accurate, and complete invoices for FFP contracts, and forward the approved invoices for payment processing. The CS will work with all involved to resolve any invoicing issues and insure the invoice documentation is accurate in the electronic record.</p> <p>The total amount of award: \$XXXX. The obligation for this award is shown in box 15G.</p>	1	LO	XXXX	XXXX

SECTION C – Statement of Work

STATEMENT OF WORK

DIGITAL MINIMALLY VIABLE PRODUCT (MVP)

1 Methodology

1.1 Discovery and Design

The contractor will work collaboratively with USCIS to determine how the problem will be solved through digitalization; utilize user centered design techniques and product management methods to create an initial product vision, product roadmap, and scope of the MVP by completing the following tasks:

1. Conduct discovery to determine a digital solution to the agency problem and end user goals for this activity.
2. Create hypothesis statement(s) that can be tested by the release of the MVP.
3. Create a product vision and initial scope for the MVP and product roadmap.

The successful solution, at a minimum, shall also include the following best practices as highlighted in the digital service playbook.

Understand what people need:

The contractor shall begin this digital service project by exploring and pinpointing the needs of the people who will use the service, and the ways the service will fit into their lives. The vendor shall continually test the products with end users to ensure delivery is focused on meeting their needs. In delivery of this effort the contractor shall:

1. Early in the project, the contractor shall spend time with current and prospective users of the service.
2. Use a range of qualitative and quantitative research methods to determine people's goals, needs, and behaviors.
3. Develop and test mock ups or prototypes of solutions with real people, in the field if possible.
4. Document the findings about user goals, needs, behaviors, and preferences.
5. Share findings with the team and agency leadership.
6. Create a prioritized list of tasks the user is trying to accomplish, also known as *user stories* to be utilized in the agile development process.
7. During development, continuously user-test the MVP to ensure it meets user needs.

1.2 Development of Minimally Viable Product

Using agile software development methods, the contractor shall develop and release to end users a minimally viable product by completing the following tasks:

1. Utilize an agile development method to write and manage epics, user stories, and acceptance criteria.
2. Conduct iteration retrospectives, release planning, backlog grooming, and other common activities associated with iterative design and agile methodologies.
3. Implement best practice methods for automated testing and code reviews.
4. Work with the agency to develop or manage continuous integration, code management processes, security, 508 compliance, privacy or any other agency policies that need to be incorporated to release the product in a live environment.
5. Test solution with end users and conduct user research activities.
6. Create and track metrics to determine whether the delivered solution meets end users' needs and solves agency problem statement to some degree.
7. As a result of the feedback provide recommendations on what should be modified in future versions of the product.

The successful solution, at a minimum, shall also include the following best practices as highlighted in the digital service playbook.

Address the whole experience, from start to finish:

The contractor shall address the different ways people will interact with USCIS services; including the actions they take online, through a mobile application, on a phone, or in person. Every encounter—whether it is online or offline— should move the user closer towards their goal. In delivery of this effort the contractor shall:

1. Understand the different points at which people will interact with the service—both online and in person.
2. Identify pain points in the current way users interact with the service and prioritize these according to user needs.
3. Design the digital parts of the service so that they are integrated with the offline touch points people use to interact with the service.
4. Develop metrics that will measure how well the service is meeting user needs at each step of the service.

Make it simple and intuitive:

Successful delivery of this contract requires that the services of and products delivered will not be stressful, confusing, or daunting. Therefore, the contractor shall build and release a digital

MVP that is simple and intuitive enough that users succeed the first time, unaided. In delivery of this effort the contractor shall:

1. Use a simple and flexible design style guide for the service.
2. Use the U.S. Web Design Standards as a default.
3. Use the design style guide consistently for related digital services.
4. Give users clear information about where they are in each step of the process.
5. Follow accessibility best practices to ensure all people can use the service.
6. Provide users with a way to exit and return later to complete the process.
7. Use language that is familiar to the user and easy to understand.
8. Use language and design consistently throughout the service, including online and offline touch points.

Use data to drive decisions:

At every stage of a project, the contractor shall measure how well the services are working for end-users. This includes measuring how well a system performs and how people are interacting with it in real-time. These metrics shall be reported to the Program Managers to find issues and identify which bug fixes and improvements should be prioritized. Along with monitoring tools, a feedback mechanism should be in place for people to report issues directly. In delivery of this effort the contractor shall:

1. Monitor system-level resource utilization in real time.
2. Monitor system performance in real-time (e.g. response time, latency, throughput, and error rates).
3. Track concurrent users in real-time and monitor user behaviors in the aggregate to determine how well the service meets user needs.
4. Provide metrics which may be published internally.
5. Provide metrics which may be published externally.
6. Use an experimentation tool that supports multivariate testing in production.

Retrospective – What worked, what didn't, what to do next:

Following the development and release of the MVP, the government and contractor team comes together to understand from a project viewpoint to identify improvement actions. In delivery of this effort the contractor shall complete the following tasks:

1. Conduct a project retrospective activity that analyzes data gathered during performance around goals, timeline, budget, major events, and success or failures.
2. Determine what roadblocks were mitigated and which ones still exist that need to be addressed.
3. Provide or update the Product Roadmap for scaling the MVP through continuous design and agile processes.

4. Ensure all system documentation, user stories, acceptance criteria and test scripts are finalized.

2 Strategies, Tactics, and Approaches for Meeting the SOO

REDACTED

3 Modern XXX XXXX

REDACTED

4 Re-Platforming the XXXX XXXX

REDACTED

5 Modern Way of XXXX XXXX

REDACTED

6 Modernization XXXX XXXX

REDACTED

7 Cloud XXX XXX

REDACTED

8 Transparent Means of XXX XXXX

REDACTED

9 Contractor Separation Notification

Deliverable	Description	Frequency of Delivery
Separation Notification	The CO and COR must be notified of each contract employee termination/resignation. (The COR will then notify the Office of Security & Integrity (OSI) Personnel Security Division (PSD) to coordinate the exit clearance forms.	Within five (5) days of each occurrence.

10 Federal Contractor Compliance with E-Verify

Within thirty (30) days of contract award, the contractor shall provide attestation to the CO that the contractor and any subcontractor employees are registered in E-Verify.

11 Place of Performance

The place of performance will be at the USCIS headquarters, 111 Massachusetts Avenue, NW Washington, DC 20529-2220 or the contractor's place of business.

12 Hours of Operation

Normal duty hours are within the hours of 6:00 am to 6:00 pm, Monday through Friday, excluding Government holidays. A current list of Federal Government holidays is located at the following website: <https://www.opm.gov/policy-data-oversight/snow-dismissal-procedures/federal-holidays/>.

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) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

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

Section 508 Applicable EIT Accessibility Standards

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

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

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

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

Section 508 Applicable Exceptions

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

Section 508 Compliance Requirements

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

Enterprise Architecture (EA) Compliance Language

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.

ISO Terms and Conditions for Sensitive but Unclassified Requests

DHS Security Policy Requirement

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

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

Encryption Compliance 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 Requirement

The following requirements should be included in all acquisition documents.

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 three 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 fourth 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 begin commencing 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 (NTP) at least one day before performance is to begin. If the Government decides to issue the NTP prior to all employees being able to perform, there will be a reduction of price based upon the offeror's prices submitted in the price breakout chart.

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.

GOVERNMENT-FURNISHED EQUIPMENT

- (a) The Government will provide contractor with the following Government Furnished Property, which is not authorized to be removed from its location unless given previous written approval by the COR:

Description of Government Property	When the GFP will be furnished	When the GFP will be returned	Acquisition cost per unit
XXXX laptops	Post award after EOD of personnel	End of period of performance or separation of a contract employee	\$XXXX

- (b) The Government will issue this equipment to no more than X contractor employees upon EOD of personnel. An additional X will be provided at a later date that has not yet been determined.

SECTION I – Contract Clauses

FAR Clauses Incorporated By Reference

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)

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)

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.]

(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).

(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).

(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]

(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).

(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).

(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]

(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).

___ (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).

___ (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 **27 months**.

(End of Clause)

52.245-1 GOVERNMENT PROPERTY (JAN 2017)

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

“Cannibalize” means to remove parts from Government property for use or for installation on other Government property.

“Contractor-acquired property” means property acquired, fabricated, or otherwise provided by the Contractor for performing a contract, and to which the Government has title.

“Contractor inventory” means—

(1) Any property acquired by and in the possession of a Contractor or subcontractor under a contract for which title is vested in the Government and which exceeds the amounts needed to complete full performance under the entire contract;

(2) Any property that the Government is obligated or has the option to take over under any type of contract, e.g., as a result either of any changes in the specifications or plans thereunder or of the termination of the contract (or subcontract thereunder), before completion of the work, for the convenience or at the option of the Government; and

(3) Government-furnished property that exceeds the amounts needed to complete full performance under the entire contract.

“Contractor's managerial personnel” means the Contractor's directors, officers, managers, superintendents, or equivalent representatives who have supervision or direction of—

- (1) All or substantially all of the Contractor's business;
- (2) All or substantially all of the Contractor's operation at any one plant or separate location; or
- (3) A separate and complete major industrial operation.

“Demilitarization” means rendering a product unusable for, and not restorable to, the purpose for which it was designed or is customarily used.

“Discrepancies incident to shipment” means any differences (*e.g.*, count or condition) between the items documented to have been shipped and items actually received.

“Equipment” means a tangible item that is functionally complete for its intended purpose, durable, nonexpendable, and needed for the performance of a contract. Equipment is not intended for sale, and does not ordinarily lose its identity or become a component part of another article when put into use. Equipment does not include material, real property, special test equipment or special tooling.

“Government-furnished property” means property in the possession of, or directly acquired by, the Government and subsequently furnished to the Contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract.

“Government property” means all property owned or leased by the Government. Government property includes both Government-furnished and Contractor-acquired property. Government property includes material, equipment, special tooling, special test equipment, and real property. Government property does not include intellectual property and software.

“Loss of Government Property” means unintended, unforeseen or accidental loss, damage or destruction to Government property that reduces the Government’s expected economic benefits of the property. Loss of Government property does not include purposeful destructive testing, obsolescence, normal wear and tear or manufacturing defects. Loss of Government property includes, but is not limited to—

- (1) Items that cannot be found after a reasonable search:
- (2) Theft:
- (3) Damage resulting in unexpected harm to property requiring repair to restore the item to usable condition; or
- (4) Destruction resulting from incidents that render the item useless for its intended purpose or beyond economical repair.

“Material” means property that may be consumed or expended during the performance of a contract, component parts of a higher assembly, or items that lose their individual identity through incorporation into an end item. Material does not include equipment, special tooling, special test equipment or real property.

“Nonseverable” means property that cannot be removed after construction or installation without substantial loss of value or damage to the installed property or to the premises where installed.

“Precious metals” means silver, gold, platinum, palladium, iridium, osmium, rhodium, and ruthenium.

“Production scrap” means unusable material resulting from production, engineering, operations and maintenance, repair, and research and development contract activities. Production scrap may have value when re-melted or reprocessed, e.g., textile and metal clippings, borings, and faulty castings and forgings.

“Property” means all tangible property, both real and personal.

“Property Administrator” means an authorized representative of the Contracting Officer appointed in accordance with agency procedures, responsible for administering the contract requirements and obligations relating to Government property in the possession of a Contractor.

“Property records” means the records created and maintained by the contractor in support of its stewardship responsibilities for the management of Government property.

“Provide” means to furnish, as in Government-furnished property, or to acquire, as in contractor-acquired property.

“Real property” See Federal Management Regulation 102-71.20 (41 CFR 102-71.20).

“Sensitive property” means property potentially dangerous to the public safety or security if stolen, lost, or misplaced, or that shall be subject to exceptional physical security, protection, control, and accountability. Examples include weapons, ammunition, explosives, controlled substances, radioactive materials, hazardous materials or wastes, or precious metals.

“Unit acquisition cost” means—

- (1) For Government-furnished property, the dollar value assigned by the Government and identified in the contract; and
- (2) For contractor-acquired property, the cost derived from the Contractor’s records that reflect consistently applied generally accepted accounting principles.

(b) *Property management.*

- (1) The Contractor shall have a system of internal controls to manage (control, use, preserve, protect, repair and maintain) Government property in its possession. The system shall be adequate to satisfy the requirements of this clause. In doing so, the Contractor shall initiate and maintain the processes, systems, procedures, records, and methodologies necessary for effective and efficient control of Government property. The Contractor shall disclose any significant changes to its property management system to the Property Administrator prior to implementation of the changes. The Contractor may employ customary commercial practices, voluntary consensus standards, or industry-leading practices and standards that provide effective and efficient Government property management that are necessary and appropriate for the performance of this contract (except where inconsistent with law or regulation).

(2) The Contractor's responsibility extends from the initial acquisition and receipt of property, through stewardship, custody, and use until formally relieved of responsibility by authorized means, including delivery, consumption, expending, sale (as surplus property), or other disposition, or via a completed investigation, evaluation, and final determination for lost property. This requirement applies to all Government property under the Contractor's accountability, stewardship, possession or control, including its vendors or subcontractors (see paragraph (f)(1)(v) of this clause).

(3) The Contractor shall include the requirements of this clause in all subcontracts under which Government property is acquired or furnished for subcontract performance.

(4) The Contractor shall establish and maintain procedures necessary to assess its property management system effectiveness and shall perform periodic internal reviews, surveillances, self assessments, or audits. Significant findings or results of such reviews and audits pertaining to Government property shall be made available to the Property Administrator.

(c) Use of Government property.

(1) The Contractor shall use Government property, either furnished or acquired under this contract, only for performing this contract, unless otherwise provided for in this contract or approved by the Contracting Officer.

(2) Modifications or alterations of Government property are prohibited, unless they are—

- (i) Reasonable and necessary due to the scope of work under this contract or its terms and conditions;
- (ii) Required for normal maintenance; or
- (iii) Otherwise authorized by the Contracting Officer.

(3) The Contractor shall not cannibalize Government property unless otherwise provided for in this contract or approved by the Contracting Officer.

(d) Government-furnished property.

(1) The Government shall deliver to the Contractor the Government-furnished property described in this contract. The Government shall furnish related data and information needed for the intended use of the property. The warranties of suitability of use and timely delivery of Government-furnished property do not apply to property acquired or fabricated by the Contractor as contractor-acquired property and subsequently transferred to another contract with this Contractor.

(2) The delivery and/or performance dates specified in this contract are based upon the expectation that the Government-furnished property will be suitable for contract performance and will be delivered to the Contractor by the dates stated in the contract.

(i) If the property is not delivered to the Contractor by the dates stated in the contract, the Contracting Officer shall, upon the Contractor's timely written request, consider an equitable adjustment to the contract.

(ii) In the event property is received by the Contractor, or for Government-furnished property after receipt and installation, in a condition not suitable for its intended use, the Contracting Officer shall, upon the Contractor's timely written request, advise the Contractor on a course of action to remedy the problem. Such action may include repairing, replacing, modifying, returning, or otherwise disposing of the property at the Government's expense. Upon completion of the required action(s), the Contracting Officer shall consider an equitable adjustment to the contract (see also paragraph (f)(1)(ii)(A) of this clause).

(iii) The Government may, at its option, furnish property in an “as-is” condition. The Contractor will be given the opportunity to inspect such property prior to the property being provided. In such cases, the Government makes no warranty with respect to the serviceability and/or suitability of the property for contract performance. Any repairs, replacement, and/or refurbishment shall be at the Contractor's expense.

(3)(i) The Contracting Officer may by written notice, at any time—

(A) Increase or decrease the amount of Government-furnished property under this contract;

(B) Substitute other Government-furnished property for the property previously furnished, to be furnished, or to be acquired by the Contractor for the Government under this contract; or

(C) Withdraw authority to use property.

(ii) Upon completion of any action(s) under paragraph (d)(3)(i) of this clause, and the Contractor's timely written request, the Contracting Officer shall consider an equitable adjustment to the contract.

(e) *Title to Government property.*

(1) All Government-furnished property and all property acquired by the Contractor, title to which vests in the Government under this paragraph (collectively referred to as “Government property”), is subject to the provisions of this clause. The Government shall retain title to all Government-furnished property. Title to Government property shall not be affected by its incorporation into or attachment to any property not owned by the Government, nor shall Government property become a fixture or lose its identity as personal property by being attached to any real property.

(2) Title vests in the Government for all property acquired or fabricated by the Contractor in accordance with the financing provisions or other specific requirements for passage of title in the contract. Under fixed price type contracts, in the absence of financing provisions or other specific requirements for passage of title in the contract, the Contractor retains title to all property acquired by the Contractor for use on the contract, except for property identified as a deliverable end item. If a deliverable item is to be retained by the Contractor for use after inspection and

acceptance by the Government, it shall be made accountable to the contract through a contract modification listing the item as Government-furnished property.

(3) *Title under Cost-Reimbursement or Time-and-Material Contracts or Cost-Reimbursable line items under Fixed-Price contracts.*

(i) Title to all property purchased by the Contractor for which the Contractor is entitled to be reimbursed as a direct item of cost under this contract shall pass to and vest in the Government upon the vendor's delivery of such property.

(ii) Title to all other property, the cost of which is reimbursable to the Contractor, shall pass to and vest in the Government upon—

(A) Issuance of the property for use in contract performance;

(B) Commencement of processing of the property for use in contract performance; or

(C) Reimbursement of the cost of the property by the Government, whichever occurs first.

(f) *Contractor plans and systems.*

(1) Contractors shall establish and implement property management plans, systems, and procedures at the contract, program, site or entity level to enable the following outcomes:

(i) *Acquisition of Property.* The Contractor shall document that all property was acquired consistent with its engineering, production planning, and property control operations.

(ii) *Receipt of Government Property.* The Contractor shall receive Government property and document the receipt, record the information necessary to meet the record requirements of paragraph (f)(1)(iii)(A)(1) through (5) of this clause, identify as Government owned in a manner appropriate to the type of property (*e.g.*, stamp, tag, mark, or other identification), and manage any discrepancies incident to shipment.

(A) *Government-furnished property.* The Contractor shall furnish a written statement to the Property Administrator containing all relevant facts, such as cause or condition and a recommended course(s) of action, if overages, shortages, or damages and/or other discrepancies are discovered upon receipt of Government-furnished property.

(B) *Contractor-acquired property.* The Contractor shall take all actions necessary to adjust for overages, shortages, damage and/or other discrepancies discovered upon receipt, in shipment of Contractor-acquired property from a vendor or supplier, so as to ensure the proper allocability and allowability of associated costs.

(iii) *Records of Government property.* The Contractor shall create and maintain records of all Government property accountable to the contract, including Government-furnished and Contractor-acquired property.

(A) Property records shall enable a complete, current, auditable record of all transactions and shall, unless otherwise approved by the Property Administrator, contain the following:

(1) The name, part number and description, National Stock Number (if needed for additional item identification tracking and/or disposition) and other data elements as necessary and required in accordance with the terms and conditions of the contract.

(2) Quantity received (or fabricated), issued, and balance-on-hand.

(3) Unit acquisition cost.

(4) Unique-item identifier or equivalent (if available and necessary for individual item tracking).

(5) Unit of measure.

(6) Accountable contract number or equivalent code designation.

(7) Location.

(8) Disposition.

(9) Posting reference and date of transaction.

(10) Date placed in service (if required in accordance with the terms and conditions of the contract).

(B) *Use of a Receipt and Issue System for Government Material.* When approved by the Property Administrator, the Contractor may maintain, in lieu of formal property records, a file of appropriately cross-referenced documents evidencing receipt, issue, and use of material that is issued for immediate consumption.

(iv) *Physical inventory.* The Contractor shall periodically perform, record, and disclose physical inventory results. A final physical inventory shall be performed upon contract completion or termination. The Property Administrator may waive this final inventory requirement, depending on the circumstances (*e.g.*, overall reliability of the Contractor's system or the property is to be transferred to a follow-on contract).

(v) *Subcontractor control.*

(A) The Contractor shall award subcontracts that clearly identify items to be provided and the extent of any restrictions or limitations on their use. The

Contractor shall ensure appropriate flow down of contract terms and conditions (e.g., extent of liability for loss of Government property).

(B) The Contractor shall assure its subcontracts are properly administered and reviews are periodically performed to determine the adequacy of the subcontractor's property management system.

(vi) *Reports.* The Contractor shall have a process to create and provide reports of discrepancies, loss of Government property, physical inventory results, audits and self-assessments, corrective actions, and other property related reports as directed by the Contracting Officer.

(vii) *Relief of stewardship responsibility and liability.* The Contractor shall have a process to enable the prompt recognition, investigation, disclosure and reporting of loss of Government property, including losses that occur at subcontractor or alternate site locations.

(A) This process shall include the corrective actions necessary to prevent recurrence.

(B) Unless otherwise directed by the Property Administrator, the Contractor shall investigate and report to the Government all incidents of property loss as soon as the facts become known. Such reports shall, at a minimum, contain the following information:

- (1) Date of incident (if known).
- (2) The data elements required under paragraph (f)(1)(iii)(A) of this clause.
- (3) Quantity.
- (4) Accountable contract number.
- (5) A statement indicating current or future need.
- (6) Unit acquisition cost, or if applicable, estimated sales proceeds, estimated repair or replacement costs.
- (7) All known interests in commingled material of which includes Government material.
- (8) Cause and corrective action taken or to be taken to prevent recurrence.
- (9) A statement that the Government will receive compensation covering the loss of Government property, in the event the Contractor was or will be reimbursed or compensated.
- (10) Copies of all supporting documentation.

(11) Last known location.

(12) A statement that the property did or did not contain sensitive, export controlled, hazardous, or toxic material, and that the appropriate agencies and authorities were notified.

(C) Unless the contract provides otherwise, the Contractor shall be relieved of stewardship responsibility and liability for property when—

(1) Such property is consumed or expended, reasonably and properly, or otherwise accounted for, in the performance of the contract, including reasonable inventory adjustments of material as determined by the Property Administrator;

(2) Property Administrator grants relief of responsibility and liability for loss of Government property;

(3) Property is delivered or shipped from the Contractor's plant, under Government instructions, except when shipment is to a subcontractor or other location of the Contractor; or

(4) Property is disposed of in accordance with paragraphs (j) and (k) of this clause.

(viii) *Utilizing Government property.*

(A) The Contractor shall utilize, consume, move, and store Government Property only as authorized under this contract. The Contractor shall promptly disclose and report Government property in its possession that is excess to contract performance.

(B) Unless otherwise authorized in this contract or by the Property Administrator the Contractor shall not commingle Government material with material not owned by the Government.

(ix) *Maintenance.* The Contractor shall properly maintain Government property. The Contractor's maintenance program shall enable the identification, disclosure, and performance of normal and routine preventative maintenance and repair. The Contractor shall disclose and report to the Property Administrator the need for replacement and/or capital rehabilitation.

(x) *Property closeout.* The Contractor shall promptly perform and report to the Property Administrator contract property closeout, to include reporting, investigating and securing closure of all loss of Government property cases; physically inventorying all property upon termination or completion of this contract; and disposing of items at the time they are determined to be excess to contractual needs.

(2) The Contractor shall establish and maintain Government accounting source data, as may be required by this contract, particularly in the areas of recognition of acquisitions, loss of Government property, and disposition of material and equipment.

(g) *Systems analysis.*

- (1) The Government shall have access to the contractor's premises and all Government property, at reasonable times, for the purposes of reviewing, inspecting and evaluating the Contractor's property management plan(s), systems, procedures, records, and supporting documentation that pertains to Government property. This access includes all site locations and, with the Contractor's consent, all subcontractor premises.
- (2) Records of Government property shall be readily available to authorized Government personnel and shall be appropriately safeguarded.
- (3) Should it be determined by the Government that the Contractor's (or subcontractor's) property management practices are inadequate or not acceptable for the effective management and control of Government property under this contract, or present an undue risk to the Government, the Contractor shall prepare a corrective action plan when requested by the Property Administrator and take all necessary corrective actions as specified by the schedule within the corrective action plan.
- (4) The Contractor shall ensure Government access to subcontractor premises, and all Government property located at subcontractor premises, for the purposes of reviewing, inspecting and evaluating the subcontractor's property management plan, systems, procedures, records, and supporting documentation that pertains to Government property.

(h) *Contractor Liability for Government Property.*

- (1) Unless otherwise provided for in the contract, the Contractor shall not be liable for loss of Government property furnished or acquired under this contract, except when any one of the following applies—
 - (i) The risk is covered by insurance or the Contractor is otherwise reimbursed (to the extent of such insurance or reimbursement). The allowability of insurance costs shall be determined in accordance with 31.205-19.
 - (ii) Loss of Government property that is the result of willful misconduct or lack of good faith on the part of the Contractor's managerial personnel.
 - (iii) The Contracting Officer has, in writing, revoked the Government's assumption of risk for loss of Government property due to a determination under paragraph (g) of this clause that the Contractor's property management practices are inadequate, and/or present an undue risk to the Government, and the Contractor failed to take timely corrective action. If the Contractor can establish by clear and convincing evidence that the loss of Government property occurred while the Contractor had adequate property management practices or the loss did not result from the Contractor's failure to maintain adequate property management practices, the Contractor shall not be held liable.
- (2) The Contractor shall take all reasonable actions necessary to protect the property from further loss. The Contractor shall separate the damaged and undamaged property, place all the affected property in the best possible order, and take such other action as the Property Administrator directs.

(3) The Contractor shall do nothing to prejudice the Government's rights to recover against third parties for any loss of Government property.

(4) The Contractor shall reimburse the Government for loss of Government property, to the extent that the Contractor is financially liable for such loss, as directed by the Contracting Officer.

(5) Upon the request of the Contracting Officer, the Contractor shall, at the Government's expense, furnish to the Government all reasonable assistance and cooperation, including the prosecution of suit and the execution of instruments of assignment in favor of the Government in obtaining recovery.

(i) *Equitable adjustment.* Equitable adjustments under this clause shall be made in accordance with the procedures of the Changes clause. However, the Government shall not be liable for breach of contract for the following:

(1) Any delay in delivery of Government-furnished property.

(2) Delivery of Government-furnished property in a condition not suitable for its intended use.

(3) An increase, decrease, or substitution of Government-furnished property.

(4) Failure to repair or replace Government property for which the Government is responsible. Standard Form 1428.

(j) *Contractor inventory disposal.* Except as otherwise provided for in this contract, the Contractor shall not dispose of Contractor inventory until authorized to do so by the Plant Clearance Officer or authorizing official.

(1) *Predisposal requirements.*

(i) If the Contractor determines that the property has the potential to fulfill requirements under other contracts, the Contractor, in consultation with the Property Administrator, shall request that the Contracting Officer transfer the property to the contract in question, or provide authorization for use, as appropriate. In lieu of transferring the property, the Contracting Officer may authorize the Contractor to credit the costs of Contractor-acquired property (material only) to the losing contract, and debit the gaining contract with the corresponding cost, when such material is needed for use on another contract. Property no longer needed shall be considered contractor inventory.

(ii) For any remaining Contractor-acquired property, the Contractor may purchase the property at the unit acquisition cost if desired or make reasonable efforts to return unused property to the appropriate supplier at fair market value (less, if applicable, a reasonable restocking fee that is consistent with the supplier's customary practices.)

(2) *Inventory disposal schedules.*

(i) Absent separate contract terms and conditions for property disposition, and provided the property was not reutilized, transferred, or otherwise disposed of, the Contractor, as

directed by the Plant Clearance Officer or authorizing official, shall use Standard Form 1428, Inventory Disposal Schedule or electronic equivalent, to identify and report—

(A) Government-furnished property that is no longer required for performance of this contract;

(B) Contractor-acquired property, to which the Government has obtained title under paragraph (e) of this clause, which is no longer required for performance of that contract; and

(C) Termination inventory.

(ii) The Contractor may annotate inventory disposal schedules to identify property the Contractor wishes to purchase from the Government, in the event that the property is offered for sale.

(iii) Separate inventory disposal schedules are required for aircraft in any condition, flight safety critical aircraft parts, and other items as directed by the Plant Clearance Officer

(iv) The Contractor shall provide the information required by FAR 52.245-1(f)(1)(iii) along with the following:

(A) Any additional; information that may facilitate understanding of the property's intended use.

(B) For work-in-progress, the estimated percentage of completion.

(C) For precious metals in raw or bulk form, the type of metal and estimated weight.

(D) For hazardous material or property contaminated with hazardous material, the type of hazardous material.

(E) For metals in mill product form, the form, shape, treatment, hardness, temper, specification (commercial or Government) and dimensions (thickness, width and length).

(v) Property with the same description, condition code, and reporting location may be grouped in a single line item.

(vi) Scrap should be reported by "lot" along with metal content, estimated weight and estimated value.

(3) *Submission requirements.*

(i) The Contractor shall submit inventory disposal schedules to the Plant Clearance Officer no later than—

(A) 30 days following the Contractor's determination that a property item is no longer required for performance of this contract;

(B) 60 days, or such longer period as may be approved by the Plant Clearance Officer, following completion of contract deliveries or performance; or

(C) 120 days, or such longer period as may be approved by the Termination Contracting Officer, following contract termination in whole or in part.

(ii) Unless the Plant Clearance Officer determines otherwise, the Contractor need not identify or report production scrap on inventory disposal schedules, and may process and dispose of production scrap in accordance with its own internal scrap procedures. The processing and disposal of other types of Government-owned scrap will be conducted in accordance with the terms and conditions of the contract or Plant Clearance Officer direction, as appropriate.

(4) *Corrections.* The Plant Clearance Officer may—

(i) Reject a schedule for cause (*e.g.*, contains errors, determined to be inaccurate); and

(ii) Require the Contractor to correct an inventory disposal schedule.

(5) *Postsubmission adjustments.* The Contractor shall notify the Plant Clearance Officer at least 10 working days in advance of its intent to remove an item from an approved inventory disposal schedule. Upon approval of the Plant Clearance Officer, or upon expiration of the notice period, the Contractor may make the necessary adjustments to the inventory schedule.

(6) *Storage.*

(i) The Contractor shall store the property identified on an inventory disposal schedule pending receipt of disposal instructions. The Government's failure to furnish disposal instructions within 120 days following acceptance of an inventory disposal schedule may entitle the Contractor to an equitable adjustment for costs incurred to store such property on or after the 121st day.

(ii) The Contractor shall obtain the Plant Clearance Officer's approval to remove property from the premises where the property is currently located prior to receipt of final disposition instructions. If approval is granted, any costs incurred by the Contractor to transport or store the property shall not increase the price or fee of any Government contract. The storage area shall be appropriate for assuring the property's physical safety and suitability for use. Approval does not relieve the Contractor of any liability for such property under this contract.

(7) *Disposition instructions.*

(i) The Contractor shall prepare for shipment, deliver f.o.b. origin, or dispose of Contractor inventory as directed by the Plant Clearance Officer. Unless otherwise directed by the Contracting Officer or by the Plant Clearance Officer, the Contractor shall

remove and destroy any markings identifying the property as U.S. Government-owned property prior to its disposal.

(ii) The Contracting Officer may require the Contractor to demilitarize the property prior to shipment or disposal. In such cases, the Contractor may be entitled to an equitable adjustment under paragraph (i) of this clause.

(8) *Disposal proceeds.* As directed by the Contracting Officer, the Contractor shall credit the net proceeds from the disposal of Contractor inventory to the contract, or to the Treasury of the United States as miscellaneous receipts.

(9) *Subcontractor inventory disposal schedules.* The Contractor shall require its Subcontractors to submit inventory disposal schedules to the Contractor in accordance with the requirements of paragraph (j)(3) of this clause.

(k) *Abandonment of Government property.*

(1) The Government shall not abandon sensitive property or termination inventory without the Contractor's written consent.

(2) The Government, upon notice to the Contractor, may abandon any nonsensitive property in place, at which time all obligations of the Government regarding such property shall cease.

(3) Absent contract terms and conditions to the contrary, the Government may abandon parts removed and replaced from property as a result of normal maintenance actions, or removed from property as a result of the repair, maintenance, overhaul, or modification process.

(4) The Government has no obligation to restore or rehabilitate the Contractor's premises under any circumstances; however, if Government-furnished property is withdrawn or is unsuitable for the intended use, or if other Government property is substituted, then the equitable adjustment under paragraph (i) of this clause may properly include restoration or rehabilitation costs.

(l) *Communication.* All communications under this clause shall be in writing.

(m) *Contracts outside the United States.* If this contract is to be performed outside of the United States and its outlying areas, the words "Government" and "Government-furnished" (wherever they appear in this clause) shall be construed as "United States Government" and "United States Government-furnished," respectively.

(End of clause)

HSAR CLAUSES IN FULL TEXT:

3052.204-71 CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

(a) *Sensitive Information*, as used in this clause, means 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.

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

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

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

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the

Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

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

(End of clause)

**ALTERNATE I
(SEP 2012)**

When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

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

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

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

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

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

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

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

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

(End of clause)

**ALTERNATE II
(JUN 2006)**

When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

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

(End of clause)

**HSAR 3052.205-70 ADVERTISEMENTS, PUBLICIZING AWARDS AND RELEASED
(SEP 2012)**

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.
- (b) All advertisements, releases, announcements, or publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

**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 3052.242-72 Contracting Officer's Technical Representative.

(End of clause)

SECTION J – List of Attachments

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

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

SECURITY REQUIREMENTS

GENERAL

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

SUITABILITY DETERMINATION

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

BACKGROUND INVESTIGATIONS

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

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

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

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

1. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"
2. FD Form 258, "Fingerprint Card" (**2 copies**)
3. Form DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
4. Position Designation Determination for Contract Personnel Form
5. Foreign National Relatives or Associates Statement
6. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
7. ER-856, "Contract Employee Code Sheet"

EMPLOYMENT ELIGIBILITY

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

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

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

CONTINUED ELIGIBILITY

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

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

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

December 31st each year, 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 v2.1*, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems (U)*, July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, *Management of Vital Records*, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

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

IT SYSTEMS SECURITY

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

employees with access to USCIS IT Systems meet the requirement for successfully completing the annual “Computer Security Awareness Training (CSAT).” All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.

CSAT can be accessed at the following: <http://otcd.uscis.dhs.gov/EDvantage.Default.asp> or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

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

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

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

SECURITY ASSURANCES

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

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

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)