U.S. Department of Homeland Security

U.S. Immigration and Customs Enforcement
Office of Diversity and Civil Rights

Program and Technical Support Services
BPA No. 70CMSD22A00000008

Attachment A - Performance Work Statement

August 15, 2022

Table of Contents

1.0 PURPOSE

This Performance Work Statement (PWS) outlines the tasks that the contractor shall provide in delivering Equal Employment Opportunity (EEO) program management.

2.0 BACKGROUND

Immigration and Customs Enforcement (ICE), through Office of Diversity and Civil Rights (ODCR), is responsible for providing equal opportunity in employment for all persons and safeguarding the civil liberties of all external stakeholders. Prohibiting discrimination in employment because of a protected basis and promoting the full realization of equal opportunity through a continuing affirmative program. To fulfill this requirement, ODCR performs the following services: processes equal employment opportunity (EEO) allegations; processes and funds reasonable accommodation (RA) requests; conducts organizational climate assessments (OCA); drafts and briefs executive and field leadership; analyzing and reports on their workforce demographics including; EEO complaints and RA trends; and other relevant data to identify and resolve barriers to equal employment, and processes harassment allegations. OCR promotes alternative dispute resolution program; creates and conducts agency-wide training; and drafts and updates equal employment policies and procedures.

3.0 SCOPE

To comply with its statutory, regulatory, Executive Order, Equal Employment Opportunity Commission (EEOC), DHS and ICE guidance, governing authority, policy, and other precedents, ODCR is seeking program support services. The Contractor shall provide knowledgeable personnel to support duties relating to the suite of the EEO stature to include EEO complaints and investigations, civil liberties, anti-harassment, disability, and reasonable accommodations programs. The government is looking for a Program Manager (PM), Program Analysts (PA), Data Analysts (DA), Technical Writers (TW), Administrative Specialist (AS) and EEO Specialists. The PAs are expected to support each program in its daily operation working alongside the federal counterpart. The PA must organize data in a manner to make it conducive to statistical reporting. The DA must be capable of collecting and arranging data from variety of sources and formats. The TW must be able to compile all data collected into a viable work product that will be presented to internal and external stakeholders.

4.0 TYPE OF CONTRACT

The government intends to issue a hybrid Firm-Fixed Price (FFP) and Labor Hour (LH) Blanket Purchase Agreement (BPA) for services.

5.0 PERIOD OF PERFORMANCE

The period of performance for the base year will be for a period of six (6) months from date of award. The option years, if exercised will be for a period of one year each with a maximum of four years. The Government may exercise the option year in accordance with the clauses herein,

however the government may de-scoped as the duties are assumed by federal government employees or the requirements no longer exists.

6.0 PLACE OF PERFORMANCE

ODCR manages its mission through a virtual (remote) work environment. All services shall be performed by the Contractor in a virtual or remote work environment. In the event work needs to be performed in person, a temporary workspace can be requested and provided at our headquarters location, 500 12th Street SW, Washington, DC.

7.0 HOURS AND DAYS OF OPERATION

Contractor employees shall generally perform all work between the hours of 7:00 a.m. and 6:00 p.m., Monday – Friday except for Federal Holidays and any other day designated by Federal Statute, Executive Order, or Presidential proclamation.

Federal Holidays

New Year's Day, January 1
Martin Luther King's Birthday, the third Monday in January
Washington's Birthday, the third Monday in February
Memorial Day, the last Monday in May
Juneteenth, June 19
Independence Day, July 4
Labor Day, the first Monday in September
Columbus Day, the second Monday in October
Veteran's Day, November 11
Thanksgiving Day, the fourth Thursday in November
Christmas Day, December 25.

8.0 CONTRACTOR PERSONNEL

All Contractor employees shall possess the applicable skill sets and educational requirements set forth in Sections 13 and 14.

9.0 KEY PERSONNEL

Contractor personnel designated as "Key Personnel" by the Government require Government acknowledgement prior to replacement. The Contractor shall submit a written notice of intent to replace the Key Personnel along with the resume' of the proposed replacement(s) to the Contracting Officer (CO) a minimum of ten (10) business days prior to the proposed date of change. To ensure that this requirement is met, the Contract shall coordinate with the Contracting Officer Representative (COR) and provide personnel resumes to facilitate the pre-approval process. The COR shall provide pre-approved selections to the (CO) of personnel replacements. The CO will provide the COR and the Contractor the final written approval of the selection.

All proposed replacement(s) shall possess qualification equal to or superior to those of the Key Personnel being replaced. Key Personnel under this BPA shall be:

1. Technical Writers
2. Program Analyst
3. Data Analyst

10.0 CONTINUITY OF SUPPORT

The Contractor shall ensure that the contractually required level of support for this requirement is always maintained. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the COR prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

11.0 CONTRACTOR EMPLOYEE CONDUCT

Employee Conduct – Contractor's employees shall comply with all applicable Government regulations, policies, and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance always and that their conduct shall not reflect discredit of on the United States of the Department of Homeland Security. The Program Manager shall ensure Contractor employees understand and abide by DHS established rules, regulations and policies concerning safety and security.

Removing Employees for Misconduct or Security Reasons – The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from this BPA for misconduct or security reasons. DHS/ICE is not a joint employer. Any request to remove a contractor employee from the contract is a remedial contract remedy. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. To the extent practical, the Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

Personnel Security Requirements - Prior to adding a new employee, the contractor will submit to the COR the employee's security application. When HQ Security provides a status on the employee's security application the COR will notify the contractor.

12.0 QUALITY

The contractor, not the Government, is responsible for quality control and management actions to meet the terms of the contract in an effective, efficient, and professional manner.

Government Oversight

The COR and/or the designated ODCR Program Manager will be responsible for monitoring the contractor's performance on specific tasks, inspecting, and accepting any work delivered. In reviewing the deliverable(s) any inadequacies in the contractor's performance will be communicated to the contractor in writing. The COR will be responsible for monitoring overall contractor's performance and reviewing and approving invoices.

The Government will evaluate the contractor's performance under this contract using through various methods to include:

1. PM/COR Inspections
2. Stakeholder Feedback

The Government will record all performance issues, whether through inspections, direct observation, customer complaint, or any other mechanism. The COR shall include an explanation of the performance issue, date of discovery, method of discovery and resolution. The COR shall schedule a meeting as soon as possible with the contractor to discuss the issue. The contractor shall rectify the substandard performance and provide an explanation of actions the contractor shall take to ensure the substandard performance does not reoccur.

13.0 TASKS AND SPECIFIC REQUIREMENTS

ODCR requires support that shall be responsible for performing the following tasks. Tasks will vary depending on the Division that the contractor is supporting. Contractors shall be available for operational planning meetings (strategic and annual reporting). Positions needed, two (2) part-time Technical Writers, three (3) Program Analysts, one (1) Administrative Specialist, (1) Program Manager, two (2) EEO Specialist, and three (3) full-time and one (1) part-time Data Analyst. The Data Analyst part time position will change to full time beginning in Option Period 1 and will continue through Option Period 4. The Technical Writers needs are subject to change throughout the option years of this contract.

13.1 - Technical Writer(s)

- Preparing briefs regarding ODCR mission activities, including identifying relevant audience and tailoring information to specific needs and areas of responsibility. Track ICE program outputs and outcomes, utilizing latest graphic design and statistical software.
- Prepare standard operating procedures.
- Assess ODCR mission activities using qualitative and quantitative data.
- Edit reports, briefs, standard operating procedures, and assessments to ensure accuracy, reviewing citations, and underlying data, and ensuring professional business standards.
- Prepare detailed data reports with trending data to ODCR senior management to be used to drive key initiatives in executive level briefings.
- Create presentations and reports from data collected from a variety of sources to drive process improvement recommendations.

13.2 - Program Analyst(s)

- Monitor the email boxes for EEO-ADR, ODCR-CRD-Chief, and Reasonable Accommodations.
- Where applicable, respond to requests and questions using ICE provided templates, regulations, and policy information.
- Route Reasonable and/or Religious Accommodations requests to the appropriate EEO specialist.
- Proactively gauge incoming email to provide escalation if needed.
- Monitor and analyze trends related to Reasonable Accommodations and Religious Accommodations requests ensuring data collected is conducive to monthly and annual reporting.
- Provide ICE Program Manager with daily, weekly, monthly, and annual reporting requirements as requested.
- If applicable, independently research program activities reviewing information, reconciling conflicting data, and recommend new and modified methods to analyze findings.
- Advise IC Program Managers of unique conditions and issues that affect program activities and recommend strategies to improve implementation and evaluation of programs.
- Provide verbal and written communication to designated team member and stakeholders in support of programmatic activities.
- Triage reasonable accommodation inbox by logging in updates and file folder creation to designated SharePoint location.
- General inbox oversight and routing; Special Emphasis Program Management (SEPM) support for sessions or training like routing surveys, collecting responses; and Women in Law Enforcement (WILE) support for tracking outcomes; weekly/monthly WAR/Data consolidation; Work collaboratively with OHC to maintain the Schedule A log.
- Create slides, videos and supporting marketing material (i.e., trifolds for the programs).

13.4 - Administrative Specialist

- Perform administrative activities for all ODCR divisions to include making copies, electronic records management, drafting and completing ad hoc reports, tracking suspense logs, and supporting ODCR employee travel.
- Coordinate ODCR's response to DHS, ICE, and external tasks by researching and gathering relevant documentation. Manage the ICE tasks system to ensure tasks are appropriately delegated within ODCR and timely responded to.
- Support for all ODCR divisions by answering internal and external telephone calls, coordinating virtual meetings (e.g., video telecommunication (VTC), Teams, and/or Webex). Check ODCR's voicemail box and complete voicemail log.
- Providing logistics and planning support for all ODCR divisions, including Special Emphasis Program observances, ODCR internal and external meeting and strategic

planning sessions, ODCR site visits, ODCR training and initiatives.

13.5 Data Analyst(s)

- Preparing reports, studies, and foundational documents regarding ODCR mission activities, including researching and compiling relevant information from multiple data sources. Analyzing data to identify trends, triggers, and barriers, and compiling information for ICE internal and external stakeholders.
- Structure large data sets to find usable information for process improvement; create presentations and reports based on best practices and recommendations.
- Support ICE Senior Leadership to identify opportunities for continual improvement; creating reports for internal teams, collaborating with individuals to collect and analyze data; use of graphs or other illustrative methods to present written findings and visualize data.
- Support the MD-715 and Barrier Analysis data pulls which include key information on reasonable, religious, and other Agency program areas.
- Conduct data pulls and prepares presentations and/or briefing packets from the data pull.
- Prepares various weekly, monthly, and quarterly reports from data collected through multiple systems as designated by the program (e.g., databases, emails, etc...)
- Provide a "How to Guide" to aid ODCR workforce on how to work with data and integration system(s). Two formal training sessions may be requested.
- Occasionally ad hoc reports that contain data pertinent to ODCR's mission.
- compilation and creation of visual representations.
- Production of visual slides of nationwide statistics for the State of the EEO. The task is performed annual. Data collected shall be arranged to maximize this reporting.
- Production of Directorate specific visual slides for the Site Visits. The task is performed annual. Data collected shall be arranged to maximize aware for the Directorate being visited.
- Production of additional ad hoc reports when requested.
- Assistance with development of job aids for formatting or artwork. Work will be situational (bi-annually).
- Assistance with Language access data usage reports from ERO, HSI, OPR, and M&A
- Data pulls supporting the MD-715 and Barrier Analysis which include key information on reasonable, religious, and other Agency program areas.

13.6 Program Manager

- Oversee daily operations of all contract employees, including coordinating work schedules, time, and attendance, assigning workload and tasks, ensuring timely completion of assignments, tracking assignment, and ensuring quality assurance by preparing timeliness and productivity metrics and reports.
- Conduct project and program management services as needed, will 'share' the workload which could include, but is not limited to drafting/writing and/or reviewing and revising process documents, briefs, reports, and assessments, providing recommendations to increase efficiency, accuracy, and standardization of ODCR services, and conducting

regular meetings with contract staff to provide guidance and track progress.
- Serve as the primary point of contact for the COR regarding daily operations, schedules, and performance; serve as the primary point of contact for the CO regarding contract administration matters.

13.7 Surge Support (EEO Specialists)

Based on the nature of supporting the Office of Diversity and Civil Rights (ODCR), there may be a need for additional support or a shift or increase in workload to meet ICE mission requirements. Operational needs such as increase in reasonable accommodation requests and investigations may result in an increase in workload.

The surge support shall be responsible for performing the following tasks.

- Responsible for monitoring the Reasonable Accommodations Email Inbox; duties include answering requests and questions using ICE provided templates, regulations, and policy information.
- Monitoring and routing Reasonable and/or Religious Accommodations requests to the appropriate EEO specialist.
- Will assist with drafting, editing, reporting, proofreading, and technical writing functions for the department.
- Oversee incoming emails to proactively gauge proper escalation if needed.
- Support the Diversity Management Division (DMD) needs for technical writing and administrative duties stemming from upcoming reasonable accommodations, religious exemption, or COVID-19 vaccination policy.
- Create and monitor trend analysis within the Office of Diversity and Civil Rights.
- Provide leadership with daily, weekly, monthly, and annual reporting requirements.
- Provide senior management with detailed data reports, evaluated information to be used in executive level briefings, trending data to drive key initiatives and highlight areas to guide policy creation.
- Independently research programmatic activities: review information, reconcile conflicting data, and devise new and modified methods to analyze findings.
- Structure large data sets to find usable information for process improvement; create presentations and reports based on best practices and recommendations.
- Advise management of unique conditions and issues that affect program activities and recommend strategies to improve implementation and evaluation of programs.
- Develop and maintain communications with team and stakeholders by providing verbal and written communication in support of programmatic activities.
- Support the MD-715 and Barrier Analysis data pulls which include key information on reasonable, religious, and other Agency program areas.

13.8 Organization Climate Assessments Survey

- Data collected needs to be compiled into a formal report. Data is complied, assessed, then summarized in a written report, from survey results only.

14.0 DESIRED KNOWLEDGE AND SKILLS

Technical Writer

- Three (3) years of demonstrated Technical Writer experience drafting, editing, and proofreading official documents for reporting purposes.
- Experience using applied research for solving complex problems.
- Experience effectively communicating with personnel at all levels of the organization and stakeholders.
- Proficiency in programs such as Adobe Illustrator or similar programs.
- Prior experience in a professional environment providing drafting, editing, reporting, proofreading, and technical writing functions

Program Analyst

- Demonstrated experience of the Reasonable and/or Religious Accommodation processes.
- Ability to independently conduct research to gather information in support of work-related projects.
- Excellent attention to detail and strong written communication skills
- Skilled in proactively identifying problems and making recommendations to management
- Researching and interpreting regulations; identifying and relaying recommendations for project success.
- Prior records management experience, including organizing electronic files, maintaining file plans, and ensuring compliance with privacy regulations.
- Prior experience with Microsoft Office suite (e.g., Outlook, Word, and Excel, as well as other analytics software.

Administrative Specialist

- Prior experience in a professional environment providing office, administrative, and technical support services.
- Prior records management experience, including organizing electronic files, maintaining file plans, and ensuring compliance with privacy regulations.
- Prior experience with Microsoft Office software, including Outlook, Microsoft Word, and Excel, as wellas other software including SharePoint, travel coordination, time and attendance, invoicing, and task management.
- Knowledge of Federal Travel Regulations (FTR)

Data Analyst

- Minimum four (4) years of demonstrated experience in collecting, analyzing, and presenting data.

- Prior experience with data management techniques to include expert trend analysis reporting.
- Skill in gathering data from multiple sources and producing a relevant statistical reporting.

Program Manager

- Three (3) years of Supervisory experience in a government office (federal, state, or local government).
- Five (5) years of Equal Employment program management experience, including the ability to apply specific EEO processes in solving complex problems and effectively communicating with personnel at all levels of the organization and stakeholders.

EEO Specialist

- Demonstrated experience with Reasonable and/or Religious Accommodation requests
- Prior experience in a professional environment providing drafting, editing, reporting, proofreading, and technical writing functions
- Ability to independently conduct research to gather information in support of work-related projects
- Excellent attention to detail and strong written communication skills
- Skilled in proactively identifying problems and making recommendations to management
- Researching and interpreting regulations; identifying and relaying recommendations for project success
- Prior records management experience, including organizing electronic files, maintaining file plans, and ensuring compliance with privacy regulations
- Prior experience with Microsoft Office software, including Outlook, Microsoft Word, and Excel, as well as other analytics software including SharePoint a plus

15.0 DELIVERABLES

The contractor shall provide monthly Task Deliverable reports. Program officers and COR may require additional special deliverables. Reports will be submitted electronically in Word or Excel formats, as necessary. Reports shall be submitted to the COR, in accordance with the requirements set forth in the PWS by written technical direction that may be issued by the CO, COR, or Program Managers.

15.1 Monthly Report

The Contractor shall provide a written monthly report no later than the 10th day of the preceding month to the COR to include, but not limited to:

1. Audit staffing and recruitment case files reviewed
2. Policy review and development

3. Respond to internal inquiries
4. Provide benefits management advice and instructions
5. Track and maintains correspondence files and documents on the share drive and SharePoint
6. Develops written analysis on various HR topics

15.2 Deliverable Table

Para	Deliverable Requirement	Performance Standard
16.0	Post Award Conference (Kick-off Meeting) Minutes	Draft due within seven (7) business days after meeting. Final version due within five (5) business days after government's review of Draft
17.0	Project Plan	Draft due at the Post Award Conference. Final version due within ten (10) business days after government's review of Draft
18.0	Transition In Plan	Five (5) business days after contract award.
19.0	Transition Out Plan	Sixty (60) calendar days prior to expiration of the order.
22.0	Quality Control Plan	Draft due within five (5) business days of award. Final version due within five (5) business days of Government's review.
26.0	Invoice Courtesy Copy	Due by the 5th business day of each Month.
13.5	Weekly Reports	Due the Monday of the following week.
13.5	Monthly Reports	Due by the 5th business day of each Month.
13.5	Quarterly Reports	Due the 2nd Monday of the next quarter.
13.5	Ad Hoc Reports	As requested within two (2) business days

16.0 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR

no later than ten (10) business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held at the Government's facility, or via teleconference.

17.0 PROJECT PLAN

The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than ten (10) business days after the Post Award Conference. The project plan shall include the vendor's proposed plan for on-boarding, staffing, scheduling, prioritizing work, and invoicing.

18.0 TRANSITION IN

The Contractor shall commence all required task order operations following a thirty (30) calendar day transition-in period. The Contractor shall provide a workforce that is fully qualified and capable of performing all work required under the task order following the thirty (30) day transition-in period. The Government will provide all cleared and vetted Contractor access to (1) post award kick-off meeting, and (2) the observance of operations in preparation for integration. The Contractor may observe personnel in performance of the program management support, adjudications support, and file management support tasks. The Contractor shall ensure during transition-in activities that it shall not interfere with productivity.

During the transition-in period, the Contractor shall become familiar with performance requirements in order to commence full performance of services on the start date following the transition-in period. The contractor shall provide a Transition-In Plan (TIP) five (5) business days after contract award that includes:

- Availability of key resources
- Timelines and proposed milestones
- Coordination with government representatives
- Review and evaluate transition of current support services
- Orientation to introduce government personnel, programs and users to the Contractors' team, tools, methodologies, and business processes
- Documentation and inventory of all government furnished equipment
- Provide briefing and personnel in-processing procedures
- Continuance of any scheduled deliverables
- Continuance of standard operations during the transition period
- Transition of records, knowledge, files, procedures and/or other designated information critical to the success of this requirement.

19.0 TRANSITION OUT

During the thirty (30) calendar day period immediately prior to the end of this contract, the contractor shall fully cooperate with government employees and any ODCR designated

personnel from other ODCR contractors to observe and become familiar with all the documentation from this contract.

The Contractor will be required to transition out all manuals, reports, and all related documentation to this task order to the successor of the following tasking order. The Contractor will be required to provide training and shadowing to the following Contractor for this task order.

The Contractor shall provide a final Transition-Out Plan as well as the support necessary to coordinate the transfer of all activities during the thirty (30) calendar day transition out period. The final Transition-Out Plan will be provided sixty (60) calendar days (or the first business day should this fall on a weekend) prior to the end of the period of performance.

The Transition-Out Plan shall include and/or address the following elements:

- Coordinate transition with DHS/ICE IT personnel
- Transfer of all software configurations in progress
- Fully support the transition of application requirements to any successor Contractor
- Technical walkthrough of the application, environment, interfaces, backlog, and help desk logs, etc.
- Transfer of all Government Furnished Equipment/Property (GFE/GFP), inventory, peripherals, software, and licenses
- Transfer of documentation currently in progress
- Briefing on all in-progress and committed items
- Provide the necessary support to ensure current and archived data is transferred to the COR including current system data, data archived to secondary storage, and related documentation generated since the contract awarded.

20.0 PROGRESS / STATUS MEETINGS

The contractor's Program Manager shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information, and resolve emergent technical problems and issues. These meetings shall take place via teleconference or at an agreed upon location between the COR and theProgram Manager.

21.0 INSPECTION AND ACCEPTANCE

All periodic reports and task deliverables shall be inspected, tested (where applicable), reviewed, and accepted by the Government within a reasonable period of time, but in no case more than 20 business days, in accordance with FAR 52.212-4, Contract Terms and Conditions—Commercial Items (Alternate I (AUG 2012). If found unacceptable, the Government shall notify the Contractor in writing or by email of the non-acceptance and detail why the deliverable was not accepted. The Contractor shall then have 10 business days to discuss, correct, or arrive at an acceptable solution with the Government.

21.1 Acceptance Criteria:

The deliverables are prepared to meet the following quality criterion:
a. All information is accurate and verifiable
b. Where appropriate, inclusion of all required steps
c. Prepared/presented all required and necessary information in an easy to follow logical, sequential manner
d. Feasibility fits into the parameters identified
e. Written in succinct, simple, straightforward language
f. Written requirements are at a consistent level of detail throughout the deliverables

22.0 QUALITY CONTROL PLAN

The offeror shall establish and maintain a complete Quality Control Plan to ensure the services in the key areas of support are performed in accordance with PWS. The offeror's proposed technical approach and commonly accepted commercial practices shall be included. The contractor shall develop and implement procedures to identify, prevent and ensure non-recurrence of defective services. The government reserves the right to perform inspections on services provided to the extent deemed necessary to protect the government's interests. The contractor must control the quality of the services and deliverables provided in support of this task and maintain substantiating evidence that services conform to contract quality requirements and furnish such information to the government if requested. A draft copy is due within five (5) business days of award. The final version is due five (5) business days after the Government's review.

23.0 FURNISHED PROPERTY GOVERNMENT

The Government will provide contractor personnel with a laptop to perform their assigned tasks. The laptop furnished by the Government to the contractor to perform work under this contract will be returned to the Government at the termination of the contract. All work performed by the contractor must be performed solely on the government issued property.

23.1 VENDOR FURNISHED PROPERTY

The vendor must provide a mobile phone for the contractor personnel.

24.0 INVOICING AND PAYMENT PROCEDURES

Contractor shall submit an invoice monthly no later than the 10th day of the month following performance. The Contractors shall submit invoices in accordance with the invoicing instructions. The Contractor shall provide an advance courtesy copy of the invoice to the COR prior to the 10th.

24.1 Invoicing Instructions:

Contractors shall use these procedures when submitting an invoice.

- Invoice Submission:

* Primary method of submission is email. Invoices shall be submitted monthly to: [redacted] Each email shall be in a .pdf format; contain only one (1) invoice and the subject line of the email will annotate the invoice number.

Note: The Contractor's Dunn and Bradstreet (D&B) DUNS number must be active in the System for Award Management (SAM) at https://www.sam.gov.

2. Content of Invoices: Each invoice submission shall contain the following information

(i) Name and address of the Contractor. The name, address and DUNS number on the invoice MUST match the information in both the Contract/Agreement and the information in the SAM.
(ii) Dunn and Bradstreet (D&B) DUNS number.
(iii) Invoice date and invoice number.
(iv) Agreement/Contract number, contract line-item number and, if applicable, the order number.
(v) Description, quantity, unit of measure, unit price and extended price of the items delivered.
(vi) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading.
(vii) Terms of any discount for prompt payment offered.
(viii) Remit to Address.
(ix) Name, title, and phone number of person to notify in event of defective invoice.
(x) Whether the invoice is "Interim" or "Final" and
(xi) ICE program office designated on order/contract/agreement.
In accordance with Contract Clause, FAR 52.212-4(g)(1), Contract Terms and Conditions – Commercial Items, or FAR 52.232-25(a)(3), Prompt Payment, as applicable, the information identified above is required with each invoice submission.

Payment Inquiries: Questions regarding invoice submission or payment, please contact ICE Financial Operations at [redacted] or by e-mail at [redacted]

In addition to the applicable clauses contained in the GSA Federal Supply Schedule 738X – Human Resource and Equal Opportunity Services, the following FAR clauses are included in this task for added emphasis of their applicability:

25.0 PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

Limiting Access to Privacy Act and Other Sensitive Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to

information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment
The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.
In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights

Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Privacy Lead Requirements

If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-t technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure

that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

PERSONAL SERVICE

DHS/ICE has determined that use of a GSA Federal Supply Schedule contract under an established agency BPA to satisfy this requirement is in the best interest of the government, economic and other factors considered, and this call/order is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled "Personal services contract".

To counter the circumstances that infer personal services and to preserve the non-personal nature of the contract, the contractor shall adhere to the following guidelines in the performance of the task:
 Contractor provides for direct supervision of all contract employees assigned to the task.
 Refrain from discussing the issues such as skill levels and hours, salaries, cost and funding data, or administrative and personnel matters affecting contractor employees with the client.
 Do not permit government officials to interview potential contractor employees, discuss individual performance, approve leave or work scheduling of contractor employees, terminate contractor employees, assist contractor employees in doing their jobs or obtain assistance from the contractor in doing Government job.
 Do not assign contractor personnel to work under direct government supervision.
 Maintain a professional distance from government employees.
 Provide contractor employees with badges, if appropriate, identifying them as contractors.
 Ensure proper communications with the government (technical discussion and government surveillance is okay, but the Government cannot tell the contractor how to do the job).
 Assign a task leader to the task order. The task leader or alternate should be the only one who accepts tasking from the assigned Government point of contact or alternative.
 The government has the right to reject the finished product or result and this does not constitute personal services.
 When travel is required for the performance on a task, the contractor personnel are only to travel as directed by their contract management.

PRIVACY ACT

Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

RIGHTS IN DATA

Any training materials, policies, procedures, timelines or other documentation, electronic work product, is the property of ICE. The contractor will not copyright, nor own exclusive rights to products developed by contractor employees in performance of this requirement. FAR 52.227-14

Rights in Data—General. (DEC 2007) is included in this call/order and added for emphasis of its applicability.

PERSONNEL SECURITY REQUIREMENTS

Prior to adding a new employee, the contractor will submit to the COR the employee's security application. When HQ Security provides a status on the employee's security application the COR will notify the contractor.

26.0 SECURITY REQUIREMENTS

GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in Contract (BPA # assigned at time of award) requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding, or terminating unescorted government facility and/or sensitive Government information access for Contractor applicants/employees, based upon the results of a Fitness screening process. ICE may, as it deems appropriate, authorize, and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the Contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable Fitness determination by the Office of Professional Responsibility (OPR), Personnel Security Operations (PSO). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable Fitness determination by OPR PSO. Contract employees are processed under DHS Instruction 121-01-007-001 (Personnel Security, Suitability and Fitness Program), or successor thereto; those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process. Sexual Abuse and Assault Prevention Standards implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003)).

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporary, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through OPR PSO. Contractor

applicant/employees nominated by a Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR PSO, through the Contracting Officer Representative (COR), within 10 days of notification by OPR PSO of nomination by the COR and initiation of an Electronic Questionnaire for Investigation Processing (e-QIP) in the Office of Personnel Management (OPM) automated on-line system.

- Standard Form 85P (Standard Form 85PS (with supplement to 85P required for those with direct contact with detainees or armed positions)), "Questionnaire for Public Trust Positions" form completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.

- Signature Release Forms (Three total) generated by OPM e-QIP upon completion of Questionnaire (e-signature recommended/acceptable). Completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.

- Electronic fingerprints taken at an approved facility **OR** two (2) SF 87 Fingerprint Cards (current revision) sent to OPR PSO. Additional information regarding fingerprints will be sent to the Contractor applicant/employee from OPR PSO.

- Optional Form 306 Declaration for Federal Employment. This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSO. Completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.

- If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards). This document is sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSO. Completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.

- One additional document may be applicable if the Contractor applicant/employee was born abroad. If applicable, the document will be sent as an attachment in an e-mail to the Contractor applicant/employee from OPR PSO. Completed online and archived by the Contractor applicant/employee in their OPM e-QIP account.

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under reciprocity. The questionnaire related to 6 CFR § 115.117 listed above in item 5 will be required for positions designated under PREA.

An adequate and current investigation is one where the investigation is not more than five years old, meets the contract risk level requirement, and applicant has not had a break in service of

more than two years. (Executive Order 13488 amended under Executive Order 13764/DHS Instruction 121-01-007-01)

Required information for submission of security packet will be provided by OPR PSO at the time of award of the contract. Only complete packages will be accepted by OPR PSO as notified by the COR.

To ensure adequate background investigative coverage, Contractor applicants/employees must currently reside in the United States or its Territories. Additionally, Contractor applicants/employees are required to have resided within the United States or its Territories for three or more years out of the last five (ICE retains the right to deem a Contractor applicant/employee ineligible due to insufficient background coverage). This timeline is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S. Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a Contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a Federal or Contractor employee position, barring any break in federal employment or federal sponsorship.

Only U.S. citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007-001. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007-001.

CONTINUED ELIGIBILITY

ICE reserves the right and prerogative to deny and/or restrict facility and information access of any Contractor employee whose actions conflict with Fitness standards contained in DHS Instruction 121-01-007-01, Chapter 3, paragraph 6.B or who violate standards of conduct under 6 CFR § 115.117. The Contracting Officer or their representative can determine if a risk of compromising sensitive Government information exists or if the efficiency of service is at risk and may direct immediate removal of a contractor employee from contract support. OPR PSO will conduct periodic reinvestigations every 5 years, or when derogatory information is received, to evaluate continued Fitness of Contractor employees.

REQUIRED REPORTS

The Contractor will notify OPR PSO, via the COR, of all terminations/resignations of Contractor employees under the contract within five days of occurrence. The Contractor will return any expired ICE issued identification cards and building passes of terminated/resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning Contractor employees under the contract to OPR PSO, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the Contractor employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR, a Quarterly Report containing the names of Contractor employees who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation). The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for Contractor payroll/voucher processing to ensure accuracy.

CORs will submit reports to [redacted]

Contractors, who are involved with management and/or use of information/data deemed "sensitive" to include 'law enforcement sensitive" are required to complete the DHS Form 11000-6-Sensitive but Unclassified Information Non-Disclosure Agreement (NDA) for Contractor employee access to sensitive information. The NDA will be administered by the COR to all contract personnel within 10 calendar days of the entry on duty date. The completed form shall remain on file with the COR for purpose of administration and inspection.

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, *DHS Policy for Sensitive Information* and ICE Policy 4003, *Safeguarding Law Enforcement Sensitive Information*."

Any unauthorized disclosure of information should be reported to [redacted]

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OPR PSO 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 OPR 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 to effect compliance with such requirements.

INFORMATION TECHNOLOGY SECURITY

When sensitive government information is processed on Department telecommunications and automated information systems, the contract company agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS MD 4300.1, *Information Technology Systems Security* (or its replacement). Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractor employees who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, regardless if the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

In accordance with Office of the Chief Information Officer (OCIO) requirements and provisions, all Contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Cybersecurity Awareness Training (CSAT) will be required upon initial access and annually thereafter. CSAT training will be provided by the appropriate component agency of DHS.

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on PALMS or by contacting [redacted] Contractor employees with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. System Administrators should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

27.0 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)

HSAR DEVIATION 15-02 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 email notification shall state the required training has been completed for all Contractor and subcontractor employees.

28.0 General Cybersecurity Contract Requirements

IMPORTANT CAUTION

Reference to contract requirements and clauses is current as of the date of publication. Due diligence should be exercised by all stakeholders in the process to confirm accuracy and applicability of the requirements identified

A.1 In accordance with ITAR 4.5.3.1 – Compliance with DHS Security Policy Terms and Conditions.

Compliance with DHS Security Policy Terms and Conditions:

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

A.2 In accordance with ITAR 4.5.3.4 and ITAR 4.5.4.4 – Security Review

Security Review Terms and Conditions

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 ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer 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 ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. 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 ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

A.3 In accordance with HSAR 3052.204-70 - Security requirements for unclassified IT resources, with ITAR 4.5.3.3 – Access to Unclassified Facilities, IT Resources, and Sensitive Information Requirement Clause Inclusion Instruction, with ITAR 4.5.3.9 – Security Requirements for Unclassified Information Technology Resources Clause, with ITAR 4.5.4.6 – Required Protections for DHS Systems Hosted in Non-DHS Data Centers, and with ITAR 4.5.4.7 – Contractor Employee Access Clause . As prescribed in (HSAR) 48 CFR 3004.470-3 **Contract clauses:**

Security Requirements For Unclassified Information Technology Resources (JUN 2006)

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

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

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

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

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

Examples of tasks that require security provisions include:

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

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

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

A.3.1 Contractor IT Security Accreditation

Contractor IT Security Accreditation

Within 6 months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (most current version) or any replacement publication, which the CO will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

A.4 In accordance with HSAR 3052.204-71 - Contractor Employee Access

Contractor Employee Access (Sep 2012)

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:

a) 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);

b) 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);

c) 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

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

e) "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.

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 CO. Upon the CO'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.

The CO 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.

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 CO. 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.

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.

A.4.1 Alternate I

Contractor IT Resource Access (Sep 2012)

1) 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.

2) 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.

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

4) 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.

5) 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:

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

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

6) 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.

A.4.2 Alternate II

Sensitive Information Limited to U.S. Citizens and Lawful Permanent Residents (JUN 2006)

1) 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.

2) 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

A.5 In accordance with White House Digital Government BYODTK – Privacy Expectations

Privacy Expectations

Government contractor employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed - through that device.

A.6 In accordance with White House Digital Government BYODTK – Mobile Information Technology Device Policy

Mobile Information Technology Device Usage

Users who conduct official DHS ICE business on a mobile IT device must:

a) Sign the Remote Access and Mobile IT Device User Agreement Form.

b) Operate the device in compliance with this policy, all applicable federal requirements, and the DHS ICE Remote Access and Mobile Information Technology Guide.

c) Not process or access Classified information on the device.

d) Use only approved and authorized DHS ICE owned devices to physically attach to DHS ICE IT systems.

e) Store only the minimum amount, if any, of Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) necessary to do one's work, and immediately delete the PII or ePHI when no longer needed. Users shall receive written approval from their supervisor before accessing, processing, transmitting, or storing DHS ICE Sensitive Information such as PII or ePHI.

f) Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.

g) Immediately contact the DHS ICE Service Desk and their immediate supervisor if the IT device is lost, stolen, damaged, destroyed, compromised, or non-functional.

h) Abide by all federal and local laws for using the device while operating a motor vehicle (e.g., users are banned from text messaging while driving federally owned vehicles, and text messaging to conduct DHS ICE business while driving non-government vehicles).

Users who are issued a DHS ICE owned mobile IT device must also:

a. Comply with DHS 4300A Sensitive Systems Handbook Attachment Q.

b. Not disable or alter security features on the device.

c. Only use the DHS ICE owned device for official government use and limited personal use.

d. Reimburse the OCIO for any personal charges incurred that are above the established fixed cost for the Agency's use of the device (e.g., roaming charges incurred for personal calls).

e. Be required to reimburse DHS ICE if the mobile IT device is lost, stolen, damaged or destroyed as a result of negligence, improper use, or willful action on the employee's part and if determined by ICE.

A.10 In accordance with HSAR Class Deviation 15-01, Special Clause, Safeguarding of Sensitive Information (MAR 2015)

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* (most current version), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (most current version), or any successor publication, and the *Security Authorization Process Guide* including templates.

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.

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.

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:

Data Universal Numbering System (DUNS).

Contract numbers affected unless all contracts by the company are affected.

Facility CAGE code if the location of the event is different than the prime contractor location.

Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email).

Contracting Officer POC (address, telephone, email).

Contract clearance level.

Name of subcontractor and CAGE code if this was an incident on a subcontractor network.

Government programs, platforms or systems involved.

Location(s) of incident.

Date and time the incident was discovered.

Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level.

Description of the Government PII and/or SPII contained within the system.

Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system; and

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:

Inspections,

Investigations,

Forensic reviews, and

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:

A brief description of the incident.

A description of the types of PII and SPII involved.

A statement as to whether the PII or SPII was encrypted or protected by other means.

Steps individuals may take to protect themselves.

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

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:

C.1 Triple credit bureau monitoring.

C.2 Daily customer service.

C.3 Alerts provided to the individual for changes and fraud; and

C.4 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*.

A.11 In accordance with HSAR Class Deviation 15-01, Special Clause, Information Technology Security and Privacy Training (MAR 2015)

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.

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.

29.0 POINTS OF CONTACT

Contracting Officer

[redacted]

Contracting Officer's Representative (COR)

[redacted]

[redacted]

Alternate Contracting Officer's Representative (COR)

[redacted]