Statement of Work

U.S. Immigration and Customs Enforcement (ICE)
Homeland Security Investigations (HSI)
Office of Administrative Operations (OAO)
April 5, 2023
Rev. June 8, 2023

1. VISION STATEMENT

Non-personal services: Acquire necessary professional contractor services in support of the ICE Homeland Security Investigations (HSI) – Office of Administrative Operations (OAO). The position(s) will report to the senior leadership within OAO.

2. INTRODUCTION

The objective of this Statement of Work (SOW) is to obtain qualified professional contract staff to support the mission of HSI. The qualified individual(s) will provide specific analytical support to the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), Office of Administrative Operations (OAO).

3. BACKGROUND

The OAO supports HSI's overall investigations through its administrative functions. More specifically, in support of the HSI investigative mission, and to ensure prompt and appropriate response to a wide variety of law enforcement information disclosure requests relating to the complex HSI investigatory portfolio and the legal processes involved, IDU addresses all information disclosure issues as they pertain to HSI. Such information disclosure matters include ICE's confidential informant (CI) program; Mutual Legal Assistance Treaty requests from foreign governments; requests from other federal, state and local agencies to assist in the furtherance of their law enforcement efforts; Congressional and special interest inquiries; litigation discovery requests; the review of statistical information relating to HSI law enforcement activities for release outside of the Department of Homeland Security (DHS); and other complex and sensitive law enforcement disclosure issues that relate specifically to HSI. IDU acts as the primary liaison for litigation issues involving information maintained by HSI and coordinates with other agencies to ensure appropriate disclosure of jointly held information pertaining to matters of mutual interest.

4. OBJECTIVE

The primary objective of this task is to obtain analytical services to support the OAO mission.

5. SCOPE

This requirement is for qualified contract employees to perform analyses as a Program Advisor, and additional support, as needed, to further the mission of HSI, as detailed above. It is anticipated that there will be sufficient effort which would require surge support on an intermittent basis. Any surge efforts will be approved for compliance with this Statement of Work by the Contracting Officer and Contracting Officer Representative (COR) who is positioned under HSI Office of Administrative Operations (OAO). The qualified individuals will provide specific analytical support to OAO. Specific tasks include

but are not limited to:

6. TASKS

- Support the Agency's litigation efforts, in coordination with Office of the Principal Legal Advisor and Assistant United States Attorneys by constructing Vaughn indices, declarations, affidavits, answers to complaints and supplemental releases.
- Research, coordinate and prepare documentation for and responses to requests for the disclosure of law enforcement information with entities within DHS and agencies outside of DHS.
- Research and review, as well as consult with law enforcement staff and make recommendations on the modification of law enforcement records in support of the DHS Traveler Redress Inquiry Program (TRIP).
- Provide subject matter expertise and requisite guidance to all HSI field and headquarters components on making sound determinations relating to the release of HSI law enforcement sensitive information.
- Draft responses to requests from other federal, state and local criminal law enforcement and regulatory agencies for a wide variety of HSI investigative and enforcement information, documents and records.
- Draft and/or edit procedural documentation relative to the dissemination and sharing of law enforcement information.
- Make recommendations to agency staff, to include HSI senior management and ICE legal staff, regarding the disclosure of HSI law enforcement information.
- Assist in the processing of requests for information relating to ICE's CI program.
- Researches, coordinates searches and prepares documentation in response to FOIA/PA requests tasked from the ICE FOIA Office for HSI information.
- Conducts thorough reviews of agency records to make initial determinations on the release of HSI law enforcement sensitive information.
- Provide technical guidance to all HSI field and headquarters components on conducting and documenting thorough searches for HSI information in response to FOIA requests.
- Supports the ICE's FOIA litigation efforts, in coordination with OPLA. ICE FOIA and Assistant United States Attorneys by assisting with the drafting of declarations, answers to complaints and supplemental releases.\
- It is anticipated that there will be sufficient effort which would require surge support on an intermittent basis. Any surge effort(s) will be approved for compliance with the Statement of Work by the Contracting Officer (CO) and Contracting Officer's Representative (COR) who is positioned under HSI/OAO.

7. NON-PERSONAL SERVICES

DHS retains the authority to make all decisions regarding the DHS mission, and the execution or interpretation of laws of the United States. Contractor services defined are not considered to be inherently Governmental in nature, as defined by Federal Acquisition Regulation (FAR) Subpart 7.5. This is a Non-Personal services contract as defined by FAR Subpart 37.101. Contractor personnel rendering services under this order are not subject to supervision or control by Government personnel. The Contractor will be responsible for the supervision of the Contractor employees at all duty locations. The Contractor is expected to work independently to accomplish the requirements of this order. The Contractor must generate reports and other deliverables as specified by the Statement of Work.

If the contractor believes that any actions constitute, or are perceived to constitute personal services, it

shall be the contractor's responsibility to notify the Contracting Officer (CO) immediately.

8. CONTRACTOR SHALL PROVIDE AND MAINTAIN QUALIFIED STAFF

The contractor shall provide and maintain qualified staff for DHS-ICE-HSI OAO who meet or exceed the standards identified below. On those occasions where personnel will need to be replaced, Contractor shall provide to the Contracting Officer Representative (COR) proposed replacement personnel within three (3) business days following vacancy of a position. The Government shall have no input as to the selection of a replacement other than to confirm that the proposed replacement meets contractual requirements.

8.1 Qualifications for Program Manager (1) (Key Personnel)

The government intends for this to be a permanent fixed price position for the duration of this requirement. Program Manager shall at a minimum:

- Paralegal/legal experience addressing disclosure related matters relating to law enforcement records
- Experience consulting with agency law enforcement and legal staff, as well as Assistant United States Attorneys, on the disclosure of law enforcement information
- Experience advising senior management on the disclosure of law enforcement sensitive information relating to litigation matters, criminal prosecutions, law enforcement exchanges, and other types of complex disclosure requests
- Ability to draft legal documents for court submission
- Program management or supervisory experience in information disclosure
- Competency in the use of all Microsoft Office products
- Experience using law enforcement databases for research
- Ten (10) years experience performing duties as a program manager or supervisor in a law enforcement organization. More than 10 years experience is preferred.

8.2 Qualifications for Management Analyst (2) (*Surge)

The government intends for these to be optional labor hour positions staffed at the discretion of the government to include surge efforts as required. The Management Analyst shall at a minimum:

- Have three (3) years of research, review and analytical experience related to addressing requests for agency information
- Have three (3) years of experience consulting with agency staff on information disclosure matters
- Have three (3) years of experience advising management on agency matters
- Exhibit proficiency in the use of all Microsoft Office products
- Have one (1) year of experience utilizing law enforcement databases for research
- Have a bachelor's degree from an accredited college or university

8.3 DHS/ICE Mandatory Training

All Contractor staff will be required to complete mandatory DHS-ICE training courses. While the list is subject to change, the topics listed below frame the current minimum requirements of the agency:

- Sexual Harassment Training
- Records Management
- Privacy Awareness
- Information Assurance Awareness Training IAAT
- Other specialized training identified by DHS or COR

DHS training shall be accomplished during contractor employee work hours and no additional compensation shall be provided. All basic training certificates are due to the COR within 60 days of the contract award or after the employee successfully enters on duty (EOD). The COR will communicate reasonable due dates for specialized training that falls outside of the mandatory DHS-ICE portfolio. The contractor shall notify the COR (via email) on an annual basis that all basic training has been kept up to date. Each employee shall abide by ICE policy and agency wide notifications to ensure they complete and maintain active training certificates.

9. PERIOD OF PERFORMANCE

The period of performance for this contract period shall be twelve (12) months from date of award with four (4) option years, as noted below.

- Base, 4 Option Periods:
  - Base Year from 1/1/20 to 12/31/20
  - Option Periods:
    - Option Year #1: 1/1/21 to 12/31/21
    - Option Year #2: 1/1/22 to 12/31/22
    - Option Year #3: 1/1/23 to 12/31/23
    - Option Year #4: 1/1/24 to 12/31/24

10. HOURS OF OPERATION

Contractor will staff OAO during normal government operating hours. For the purposes of this task, normal government operating hours are defined as: Monday through Friday with duty core hours between 8:00 am - 6:00 pm, excluding Government Federal Holidays. However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays due to an emergency requirement, to fulfill the requirements under this Statement of Work. These facilities shall only be used in performance of this contract. Performance of work under this contract in alternate Government work spaces or at home via telework, is currently not authorized. The contracting officer, COR, and program office reserve the right to authorize telework if so desired.

The following Government holidays are normally observed by Government and contractor personnel: New Year's Day, Martin Luther King's Birthday, Presidential Inauguration Day (metropolitan DC area only), President's Day, Memorial Day, Juneteenth, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas Day. Contractor personnel also observe building closures during inclement weather and any other day designated by Federal Statute, Executive Order and/or Presidential Proclamation in which the government duty station/facility is closed.

11. TRAVEL

Travel may be required to support training efforts. Contractor personnel may be asked to travel to conferences/trainings throughout the United States. Travel expenses will be reimbursed based on Federal Travel Regulations and the per diem rates established by the General Service Administration for meals and incidental expenses.

Within ten (10) calendar days of completing travel, a completed travel voucher and receipts should be submitted to the COR. All travel receipts shall be submitted with the monthly invoices for COR approval and payment. Funds allocated for travel should be annotated as travel cost and expenses on the related invoice.

12. DELIVERABLES

The contractor shall provide deliverables as described within this SOW. The delivery schedule for deliverables is outlined below. The format has either been identified in the SOW or will be determined during the post-performance conference following award.

ITEM	DELIVERABLE	FREQUENCY / DUE BY	DISTRIBUTION
1	Post Award Conference / Meeting Minutes	Will be conducted within 7 calendar days following award of the task order. Meeting minutes due 15 calendar days after meeting	Government Program Manager / COR / Contracting Officer
2	DHS/ICE Training	Certificates due to the COR within 45 days of employee onboarding or as	COR
3	Monthly Activity / Status Report	Due by the 5th business day of each month	Government Program Manager / COR
4	Time sheets/Monthly Time Card Reports for Labor Hours Contractors	Due by the 5th business day of each month	Government Program Manager / COR
5	Monthly invoices	Due by the 5th business day of each month	COR
6	Documents, Recommendations and/or Reports	As Required	Government Program Manager / COR

12.2 Post-award Conference

The purpose of the conference is to aid both Government and Contractor personnel to:
1. Achieve a clear and mutual understanding of all contract, management, and technical requirements.
2. To identify and resolve potential problems

13. GENERAL REQUIREMENTS

13.1 Place of Performance

The place of performance will be at the Government's facility located at:

U.S. Department of Homeland Security
Immigration and Customs Enforcement
500 12th Street, S.W.
Washington, D.C. 20536

13.2 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 on the United States or the DHS. The Program Manager shall ensure Contractor employees understand and abide by DHS established rules, regulations and policies concerning safety and security.

13.3 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the CO), require the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The CO will provide the Contractor with a written explanation to support any request to remove an employee.

13.4 Accident Report Procedures

In the event of an accident on Government property, or involving Government personnel or property, the Contractor shall submit a report within seventy-two (72) hours to the CO in letter form that shall include the following: (1) the time and date of the occurrence; (2) the place of occurrence; (3) a list of personnel directly involved; and (4) a narrative or description of the accident to include a chronological order of the accident and circumstances.

13.5 Contract Progress Meetings and Teleconferences

The CO, COR and Government Program Manager as appropriate, will meet periodically or participate in teleconferences with the Contractor to review the contract performance, progress, and resolve technical issues. Minutes of the meetings/teleconferences, with action items identified, shall be documented by the Contractor and provided to the COR no later than seventy-two (72) hours after meeting.

13.6 Release of Information

Contractor access to proprietary and privacy act information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information. Contractor and subcontractors shall not hold any discussions or release any information relating to this contract to anyone not having a direct interest in performance of this contract, without written consent of the CO. This restriction applies to all news releases of information to the public, industry or Government agencies, except as follows: Information for actual or potential subcontractors or other individuals necessary for Contractor's performance of this contract. Contractor and subcontractors shall not issue advertisements about projects performed under this task without

government review and approval. For the purposes of this paragraph, advertisement is Contractor-funded promotional brochures, posters, tradeshow handouts, world-wide-web pages, magazines, or any other similar type promotions.

13.7 Government Furnished Equipment and Property

The Contractor shall keep and maintain an inventory of Government-furnished equipment, which shall be made available to the COR upon request. The Contractor will be provided with desk space, telephone, general office supplies and computer workstations with ICE LAN/Internet access. No alterations shall be made to the facilities. The Contractor shall return the facilities to the government in the same condition as received, fair wear and tear excepted. These facilities shall only be used in performance of this contract. Contractor will be provided with duty hour's access to appropriate ICE workspaces. After-hours access to ICE workspace will be permitted as designated by and approved by the COR or Government Program Manager in advance of a communicated need.

13.8 Non-disclosure Statement

Any information made available to the Contractor by the Government shall be used only for carrying out the provisions of these tasks and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of these tasks. Contractor personnel shall sign Non-Disclosure statements (DHS Form 11000-6).

13.9 Conflict of Interest Avoidance

The Contractor shall notify the COR in writing no later than twenty-four (24) hours after occurrence of any potential conflicts of interest through their performance on this contract. The COR will immediately notify the CO of any potential Contractor conflicts of interest.

13.10 Invoice Requirements

Vendor invoices should be submitted on a monthly basis to the COR, A-COR, and designated finance center for all services performed. A standard timecard template or monthly timesheet report shall be provided by the contractor and verified by the COR for labor hours contractors assigned to this contract. The timecards/monthly timesheet report should be included with the monthly invoices. The contractoris responsible for reviewing and approving hours worked prior to submitting monthly invoices. Government personnel are not responsible or authorized to approve contractor reported working hours or leave. The timecard template/monthly timesheet report should align with the monthly billing period and is intended to be a consolidated summary of all timecard activity. At a minimum; this summary report should highlight the regular duty hours performed and leave taken during the respective billing period for each labor hours contract line.

14. TRANSITION/PHASE-OUT PLAN/INSTRUCTIONS

Within ninety (90) days of government notice or the final performance date, the Contractor shall present a high-level transition out plan including major milestones for transitioning support responsibilities of all tasks over to the Government/New Contractor. These activities should include as part of the transition the Inventory and orderly transfer of all Government-Furnished Equipment / Property and the transfer of documentation currently in process. In summary, the transition out plan shall also include

documentation of all current work and processes and coordination necessary to transfer of all work responsibilities to the Government or new Contractor.

The Contractor's transition out plan shall be approved by DHS ICE and shall contain a milestone schedule of events and process/system turnovers. The transition plan shall provide for the transition of all work, with no disruption in operational services. To ensure the necessary continuity of services and to maintain the current level of support, ICE will retain services of the current Contractor for the transition period, if required.

The Transition Out Plan, at a minimum, shall include:

-

TOP Workgroup, key staff (federal and/or contractor) required to transition all work for each task

- Timeline for working group and subgroups based on major milestones for transitioning all work
- A list of any deliverables necessary to ensure a smooth transition between Government/Contractor, beyond those listed below, or in Deliverables.

At the minimum, deliverables shall include all software systems, tools, and/or products developed under the contract, or SOPs/written guidelines necessary to utilize systems/tools/products and follow government processes. However, the contractor shall recommend additional deliverables to ensure a smooth transition such as administrative actions required or taken during transition, a list of resolved and unresolved transition issues, risk assessment, and lessons learned report of transition activities and recommendations.

- Communication Plan to outline how, who, what, and when appropriate information is communicated to the government/contractor.
- Quality and/or Technical Training consideration to ensure that necessary TOP workgroup members are prepared in different stages of the transition and that all planned training/briefings/recaps are complete to ensure successful transition.

When applicable, during the thirty (30) calendar day period immediately prior to the end of the contract (if the incumbent is not awarded the subsequent contract for this service), the Contractor shall permit the successor Contractor (and the successor Contractor's employees) to observe and become familiar with any and all operations under the contract. The Contractor shall fully cooperate with the successor Contractor and the Government so as not to interfere with their work or duties.

15. SECURITY REQUIREMENTS

DHS has determined that performance of the tasks as described in this SOW requires that the Contractor, subcontractor(s), vendor(s), 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 employees to commence work temporarily prior to the completion of the 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 a 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 Operation (PSO). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable Fitness determination by the OPR PSO. Contract employees are processed under the DHS Instruction 121-01-007-001 (Personal 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

Contract 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 the OPR PSO Contractor applicant/employees nominated by the Contracting Officer Representative for consideration to support this contract shall submit the following security vetting documentation to OPR PSO, through the 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.:

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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 currently have an adequate, current 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 psu-industrial-security@ice.dhs.gov

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 ICE.ADSEC@ice.dhs.gov.

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 the OPR- PSO 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 CO of the proper action to be taken to effect compliance with such requirements.

Information Technology Security Clearance

When sensitive government information is processed on Department telecommunications and automated information systems, the contractor 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 ICE.ADSEC@ice.dhs.gov. 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).

General Cybersecurity Contract Requirements

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.*

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.

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 20 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.

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.

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.

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

POINTS OF CONTACT

COR
[redacted]
DHS/ICE
500 12th Street, SW
Washington, D.C. 20024
[redacted]

HSI Program/Task Manager
[redacted]
DHS/ICE
500 12th Street, SW
Washington D.C. 20024
[redacted]

DHS/ICE/OAQ Contracting Officer
[redacted]
Contracting Officer
Office of Acquisition Management
500 12th Street, SW
Washington, D.C. 20024
[redacted]

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-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.

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.

(End of clause)