ENVIRONMENTAL HEALTH AND SAFETY SUBJECT MATTER EXPERT SUPPORT SERVICES FOR THE DEPARTMENT OF HOMELAND SECURITY OFFICE FOR CIVIL RIGHTS AND CIVIL LIBERTIES

STATEMENT OF WORK

1 BACKGROUND

The U.S. Department of Homeland Security (DHS), Office for Civil Rights and Civil Liberties (CRCL), is responsible for investigating complaints filed pursuant to 6 U.S.C. § 345 and 42 U.S.C. § 2000-ee-1, alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by DHS employees and officials, as well as contractors used by the Department or its Components. CRCL's Compliance Branch is responsible for investigating these complaints. CRCL is also charged with overseeing compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by DHS programs and activities.

2 SCOPE

2.1 The purpose of this contract is to obtain Environmental Health and Safety Subject Matter Expert (SME) Services to assist CRCL in performing its investigatory and oversight functions. The selected subject matter expert shall primarily assist CRCL in conducting investigations involving environmental health and safety issues in immigration detention facilities used by U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP), which shall include preparing reports related to the investigations. CRCL cannot precisely predict the number of facilities or the locations facilities that may require onsite reviews because it depends on the complaints received, but CRCL typically performs 10-15 onsite investigations each year. The expert may also be asked to assist CRCL with other CRCL matters related to environmental health and safety, including reviews initiated by DHS leadership, consulting with substantive work groups, providing training, or other activities as requested.

2.2 Environmental Health and Safety SME services are required to evaluate complaints received pursuant to 6 U.S.C. § 345 and 42 U.S.C. § 2000-ee-1 and also to oversee compliance with constitutional, statutory, regulatory, policy, and other requirements related to civil rights and civil liberties. In addition to evaluating complaints, the contractor shall provide assistance related to activities that arise within CRCL's authority, including, but not limited to research, analysis, and/or development of system-wide standards, policies, procedures, and training. Services include, but are not limited to, conducting reviews of DHS facilities, providing training related to their areas of expertise, and other activities and projects related to environmental health and safety concerns, as tasked by CRCL, such as participating in work groups, developing or presenting briefings, and preparation of documents. In particular, the

experts shall also be required to prepare detailed reports regarding their observations and findings, as well as to provide recommendations based upon applicable correctional standards. CRCL cannot precisely predict the extent of the related activities required because it depends on the complaints received.

3 REQUIREMENTS/TASKS

3.1 The Contractor personnel shall review, evaluate, and report on environmental health and safety issues and advise CRCL on how Department policies and practices impact various issues involving immigration detention facilities.

3.2 The Contractor personnel shall document their findings and recommendations in well written, comprehensive reports for each investigation or assignment. The Contractor personnel shall collaborate with CRCL as necessary to make edits to the written reports in order to fulfill CRCL's needs, goals, and requirements.

3.3 The Contractor personnel shall provide CRCL with guidance on various violations of civil rights or civil liberties related to environmental health and safety practices upon request, whether related to a CRCL investigation, or related to a broader CRCL issue or area of work. The Contractor personnel shall provide such guidance, whether planned or ad hoc, by telephone, email, formal report, or in person, as requested by CRCL. The guidance shall include, but not be limited to, discussions and assessments of individual cases, findings from onsite investigations, discussion of policies and practices, and any other relevant information that may arise during the course of an investigation or other aspects of CRCL's oversight work.

4 CONTRACTOR PERSONNEL

4.1 QUALIFIED PERSONNEL

The Contractor shall provide qualified environmental health and safety consultants to perform the requirements specified in this Statement of Work.

4.2 MINIMUM REQUIREMENTS FOR AN ENVIRONMENTAL HEALTH AND SAFETY SUBJECT MATTER CONSULTANT

4.2.1 The Contractor shall have a Bachelor's Degree in environmental health and safety or the natural sciences, and must hold accreditation as a Registered Sanitarian or Registered Environmental Health Specialist, with the National Environmental Health Association or a State accrediting agency.

4.2.2 The Contractor shall have at least five (5) years of direct experience with environmental health and safety working in a detention setting.

4.2.3 The Contractor shall be familiar and have experience applying the certifications or special training related to applying the American Correctional Association Standards.

4.2.4 The Contractor shall have experience investigating, auditing, or otherwise evaluating detention facilities for adherence to applicable standards related to environmental care programs and systems.

4.2.5 The Contractor shall have experience objectively critiquing environmental health and safety conditions within a detention setting.

4.2.6 The Contractor shall have experience serving as a subject matter expert providing advice, guidance, or testimony on the operation of environmental health and safety programs or systems in a detention setting.

4.2.7 The Contractor shall have experience formulating recommendations or other steps to address issues, violations, or concerns identified as part of an investigation or other type of inquiry.

4.2.8 The Contractor shall have experience applying the American Correctional Association (ACA) Standards, National Commission on Correctional Health Care (NCCHC) Standards, and other standards related to environmental health and safety issues in a detention setting.

4.2.9 The Contractor shall have knowledge and experience with the history, policies, and protocols of environmental health and safety issues in a detention setting and will be apprised of recent trends and developments in providing these services.

4.2.10 The Contractor shall have experience producing written reports that evaluate detention standards, systems, and actions present in detention facilities. This will include analysis of and application of standards and policy.

4.2.11 The Contractor shall demonstrate the ability to produce comprehensive reports that are well-written, clear, and cite relevant resources.

4.2.12 The Contractor shall demonstrate the ability to review large amounts of documentary evidence in short timeframes and provide oral briefings, written reports, and training under tight timelines.

4.2.13 The Contractor personnel must be able to travel to various locations nationwide to perform onsite investigations for several consecutive days, and work efficiently and cooperatively under the direction of CRCL personnel.

4.3 ENHANCING FACTORS

4.3.1 The Contractor has more than ten (10) years of direct experience with environmental health and safety working in a detention setting.

4.3.2 The Contractor has experience managing food service, laundry operations, or other aspect of detention operations related to environmental health and safety.

4.3.3 The Contractor has demonstrated experience in a variety of types of detention settings and with a variety of populations. The variety could include working with adults and children, working in prisons, jails, or another type of facility, or working with other special populations.

4.3.4 The Contractor has conducted and published research or written analysis regarding system-wide issues related to conditions of detention.

4.3.5 The Contractor has worked directly with the ICE National Detention Standards (NDS), Performance Based National Detention Standards (PBNDS), or other related policies governing environmental health and safety issues in immigration detention.

4.3.6 The Contractor has reviewed and evaluated environmental health and safety issues in in an immigration detention facility.

4.3.7 The Contractor has multiple key personnel who meet the minimum requirements in the statement of work.

4.4 REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

The Government may, at its sole discretion, direct 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 this contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to end services.

4.5 KEY PERSONNEL

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced. The Contractor shall not replace *Key* Contractor personnel without acknowledgment from the Contracting Officer. The Environmental Health and Safety Consultant is designated as *Key* by the Government for this requirement.

4.6 NOTICE REGARDING APPEARANCE OF CONFLICT

The nature of the work under this contract includes circumstances where Contractor personnel will likely investigate allegations and/or complaints pertaining to environmental health and safety issues within DHS Components. Contractor personnel either currently providing work for a DHS Component that is the same or similar in scope to the requirement under this contract, or who have provided the same or similar work for a DHS Component in the three years prior to the

start of this contract, are not eligible to perform services on this contract in order to prevent the existence or appearance of conflicting roles that might affect a contractor's judgement.

The Contractor shall not employ any person under this contract who is an employee of the United States Government if that employment would, or would appear to, cause a conflict of interest. The Contractor shall notify the Contracting Officer and Contracting Officer's Representative by telephone and in writing within 72 hours when a conflict of interest arises during the course of carrying out the duties of this contract.

5. POST AWARD MEETING

The Contractor shall participate in a Post Award Meeting with the Contracting Officer and the COR no later than five (5) business days after the date of award. The purpose of the Post Award Meeting is to discuss the contracting objectives of this contract. The Post Award Meeting will be held at the Government's facility or via teleconference or conference call.

6. GENERAL REPORTING REQUIREMENTS

The contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS Microsoft Office applications.

6.1 PROGRESS REPORTS

The Project Manager (Contractor) shall provide progress reports as needed to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including an assessment of technical progress, written and analytical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

6.2 PROGRESS MEETINGS

The Contractor shall be available to meet with the COR or CRCL POC upon request to present deliverables, discuss progress, exchange information and resolve emergent problems and issues. These meetings shall take place at the Government's facility or via telephone or email.

7 INTELLECTUAL PROPERTY

All reports generated, documentation produced, and research conducted in the performance of this requirement shall be the property of DHS.

8 PROTECTION OF INFORMATION

Contractor access to information protected under the Privacy Act is required under this contract. Contractor access to unclassified Security Sensitive Information and Law Enforcement Sensitive information will be required under this contract. This documentation will be provided to the Contractor in person, by mail, or by email. Contractor employees shall safeguard this

information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

The Contractor shall be required to submit a signed Non-Disclosure Agreement hereby incorporated as "Non-Disclosure Agreement."

9 GOVERNMENT FURNISHED RESOURCES

The Contractor will be furnished with Security Sensitive information for review and analysis. This documentation will be provided to the contractor in person, by mail courier, or by email. The Contractor shall safeguard this information against unauthorized disclosure or dissemination. Further, the Contractor will be furnished with DHS Laptops.

10 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment, and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in this Statement of Work.

SECTION III – DELIVERIES AND PERFORMANCE

1 PERIOD OF PERFORMANCE

The period of performance for work performed under this contract consists of a one-year base period of performance, and four (4) one-year optional periods of performance.

2.0 PLACE OF PERFORMANCE

The primary place of performance shall be the contractor's office or Contractors remote location. The Contractor shall also perform work onsite or virtually at locations to be determined by CRCL.

3.0 DELIVERABLES AND DELIVERY SCHEDULE

The Contractor shall ensure, and that Government will review all draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance with government policies, regulations, laws and directives. Written documents shall be concise and clearly written.

Final documentation deliverables shall be provided in hard and soft copy using MS Office applications. Daily, weekly and interim information deliverables and working-copy products may be provided by email or disk, as arranged with the COR.

The government will have ten (10) business days to accept or reject contract deliverables. If a deliverable is rejected and returned to the Contractor for revision, the Contractor shall provide the corrected deliverable within five (5) business days of notification of the request for revision.

All deliverables shall be submitted to the COR and assigned CRCL POC identified in this contract. A copy of the Monthly Performance Report shall be submitted to the COR and the Contracting Officer.

3.1 Deliverables

The Contractor shall provide the deliverables identified in the table below in electronic format. Electronic copies shall be delivered via email attachment or other media by mutual agreement of the parties. All electronic deliverables shall be prepared using Microsoft applications in formats selected by the Contractor. All deliverables shall be delivered via email to the COR, the Assigned CRCL POC and to the Contracting Officer, as indicated below. The Contractor's deliverables shall not contain any identifiable corporate markings.

ITEM	DELIVERABLE / EVENT	DUE BY
1	**Post Award Meeting**	5 business days of date of award.
2	**Progress Reports**	3 business days following request.
3	**Draft Investigative Reports**	**COR CHECKPOINT** Within 10 business days of receipt of assignment or completion of investigative work: Contractor shall submit draft to COR and assigned CRCL POC for review. The Contractor and CRCL will discuss the draft report to ensure its accuracy. CRCL will furnish comments and edits to Contractor who shall be responsible for making changes to the draft. **The COR must be copied on all assignment correspondence.**
4	**Oral Briefings and Ad Hoc Reports or Project-related work**	**COR CHECKPOINT** Due date to be determined by COR and/or assigned CRCL POC and Contractor.
5	**Edits to Reports and Documents**	5 business days after receipt of government comments.

4.0 GOVERNMENT ACCEPTANCE PERIOD

The COR and assigned CRCL POC will review deliverables prior to acceptance and provide the contractor with an e-mail that conveys acceptance or documented reasons for non-acceptance. The COR or assigned CRCL POC will have ten (10) business days to review deliverables and provide notification of acceptance or rejection.

SECTION IV – CONTRACT ADMINISTRATION DATA

1 KICK-OFF MEETING

The Contractor shall attend a Kick-Off meeting with the COR and members of the Program Office no later than 5 business days after the date of award. The purpose of the Kick-Off meeting, which will be chaired by the COR, is to discuss the technical objectives of this contract. The Kick-Off meeting will be held at the Government's facility, located in Washington, DC or by conference call. The specifics of the meeting will be provided upon contract award.

2 CONTRACTING OFFICER

The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds and authorize revisions of the terms and conditions of this contract. The Contracting Officer shall authorize any such revision in writing.

The Contracting Officer is:

The Contract Specialist is:

3 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The Contracting Officer will designate in writing a Contracting Officer's Representative (COR) to assist in monitoring the work under this contract. The COR is responsible for the technical administration of the contract and technical liaison with the Contractor. The COR is not authorized to change the scope of work or specifications as stated in the contract, to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract price, delivery schedule, period of performance, or other terms or conditions. The Contractor will receive a copy of the COR Appointment Letter outlining the roles and responsibilities of the COR.

The COR for this contract is: Celia Gordon / celia.gordon&hq.dhs.gov

SECTION V - INVOICE AND PAYMENT PROVISIONS

1 INVOICES

Invoices shall be prepared in accordance with FAR Clauses 52.232-7 Payments under Time-and-Materials and Labor-Hour Contracts. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

a) Cover sheet identifying DHS;
b) Contract Number;
c) Modification Number, if any;
d) DUNS Number;
e) Month services provided
f) CLIN and Accounting Classifications
g)

The Contractor shall submit one invoice by the 5th day of each month.

Contract Line Item Number (CLIN) for each billed item:

a) Time and Materials and Labor Hour – Invoices shall be submitted no more than once per month and shall be received no later than the 5th of each month (or as otherwise approved by the COR) following the services provided. The Contractor shall indicate the associated CLIN, dollar amount invoiced, and service completed. All invoices shall include the current amount billed along with a cumulative amount billed and remaining balance.

The Contractor shall submit the invoice electronically to the address below:

E-mail: [redacted]

The Contractor shall simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

a) ATTN: Office of Procurement Operations [redacted] (Contract Specialist)

   E-mail: [redacted]

b) ATTN: Office of Procurement Operations [redacted] (Contracting Officer)

   E-mail: [redacted]

c) ATTN: Office of Civil Rights and Civil Liberties [redacted] (COR)

E-mail: [redacted]

SECTION VI – SPECIAL CONTRACT REQUIREMENTS

1 CONTRACTOR PERSONNEL SECURITY CLEARANCE REQUIREMENT

All contractor and subcontractor personnel are required to complete a suitability/background investigation with the DHS Office of Security, Personnel Security Division.

The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process suitability/background investigations and suitability determinations, as required, in a timely and efficient manner.

Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, 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 suitability/background investigation to be conducted. All suitability/background investigations will be processed through the DHS Office of Security Office/PSD. Prospective Contractor employees shall submit the following completed forms to the DHS Office of Security Office/PSD. The Standard Form (SF) 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Office of Security Office/PSD no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

a) Standard Form (SF) 85P, "Questionnaire for Public Trust Positions"
b) FD Form 258, "Fingerprint Card" (2 copies)
c) DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
d) DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Office of Security/PSD. Specific instructions on submission of packages will be provided upon award of the contract.

DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a

Government facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and nonrecurring meetings in order to begin transition work.

The DHS Office of Security/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer's Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated suitability/background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not 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).

2.0 SECURITY OFFICE CONTACT

Office of Security/PSD
Customer Service Support
Washington, DC 20528
Telephone: [redacted]
E-mailbox: [redacted]

3.0 NON-DISCLOSURE AGREEMENT

The Contractor shall submit an executed Non-Disclosure Agreement (Attachment A) for each individual performing under this contract. The Contractor shall submit copies of the Non-Disclosure Agreement to the Contracting Officer and COR prior to an individual beginning performance under this contract.

4.0 DISCLOSURE OF INFORMATION

Information furnished under this contract may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personnel information must be clearly marked. Marking of items will not necessarily preclude disclosure when DHS or the Government determines disclosure is warranted by FOIA. However, if such items are not marked, all information contained within the submitted documents will be deemed to be releasable.

Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the provisions of this contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.

In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees.

Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 USC 641.

5.0 NOTIFICATION OF CONSULTING, TEACHING, SPEAKING, AND WRITING ACTIVITIES

Contractor employees shall notify the Contracting Officer's Representative before engaging in consulting, teaching, speaking, or writing activities if:

The information conveyed through the activity draws substantially on knowledge or official data that are nonpublic information as defined in 5 C.F.R. § 2635.703(b);

the subject of the activity deals in significant part with work performed under the contract; or

the subject of the activity deals in significant part with any ongoing or announced policy, program, or operation of the agency.

Notice shall be provided at least seven days prior to engaging in the activity. The scope of the notification is not intended to include work in the expert's area of expertise that does not derive from work done for DHS.

6.0 DISCLOSURE OF INFORMATION LITIGATION

Contractor employees shall comply with 6 C.F.R. Part 5, Subpart C, including 6 C.F.R. §§ 5.44 and 5.49. Those regulations generally prohibit contractor employees from testifying in connection with litigation based upon information acquired in the scope and performance of their official Department duties, except as authorized by the Department.

7.0 NON-PERSONAL SERVICES

The services required under the contract constitute professional support services, which are essential to the mission but not otherwise available within. The Government will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual Contractor employees. It shall be the responsibility of the Contractor to manage their employees and to guard against any actions that have the nature of personal services, or give the perception of personal services. If the Contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's further responsibility to notify the Contracting Officer immediately.

These services shall not be used to perform work of a policy/decision making or management nature. All decisions relative to programs supported by the Contractor will be the sole responsibility of the Government. Support services will not be ordered to circumvent personnel ceilings, pay limitations, or competitive employment procedures

8.0 EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

All Contractor employees shall identify themselves as contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages.) and display the Government-issued badge in plain view above the waist at all times.

9.0 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 at all times and that their conduct shall not reflect discredit on the United States or the DHS. The Project Manager shall ensure Contractor employees understand and abide by DHS established rules, regulations, and policies concerning safety and security.

10.0 REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

The Government may, at its sole discretion, direct 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 Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

11.0 OTHER APPLICABLE CONDITIONS

11.1 Security

Contractor access to unclassified, but Sensitive Security Information (SSI) or Personally Identifiable Information (PII), may be required under this contract. Contractor staff members shall safeguard this information against unauthorized disclosure or dissemination. Contractor staff members are not required to have a security clearance; however, a background investigation and a suitability determination will be conducted on contractor personnel assigned to this contract.

11.1.1 Protection of Information

Contractor access to sensitive but unclassified 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. The Contractor shall ensure that all Contractor personnel having access to business or procurement-sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

11.1.2 Contractor Employee Access

Sensitive Information, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or 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

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

"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 Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures. The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

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) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.
b) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR 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 COR, 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.

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

d) 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.

- 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:
    - The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
    - There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
    - The waiver must be in the best interest of the Government.

e) 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.

11.1.3 Personal Identification Verification (PIV) Credential Compliance

Authorities:

- HSPD-12 "Policies for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-06-16 "Acquisition of Products and Services for Implementation of HSPD-12"
- NIST FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- NIST SP 800-63 "Electronic Authentication Guideline"

OMB M-10-15 "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

(b) *Security Training Requirements.*

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

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor

employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

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

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)