U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 9, 2015

MEMORANDUM FOR: Heads of the Contracting Activities
Component Acquisition Executives

FROM: Soraya Correa
Chief Procurement Officer

SUBJECT: Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information

1. Introduction:

This class deviation from the Homeland Security Acquisition Regulation (HSAR):

(a) Announces two new DHS special clauses, Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015). These special clauses shall be included in Section H - Special Contract Requirements or in the clause section of the solicitation and contract;

(b) Expands the applicability of HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology Resources (JUN 2006) and 3052.204-71, Contractor Employee Access (SEP 2012); and

(c) Removes and reserves HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources (JUN 2006) when DHS special clause Safeguarding of Sensitive Information (MAR 2015) is included in the solicitation and contract.

2. Background:

The protection of sensitive information (whether electronic or paper) and the security of information technology (IT) systems that process, store or transmit this information is critical to the DHS mission. IT systems are subject to threats that can compromise the confidentiality, integrity or availability of sensitive information, adversely affecting DHS operations, assets and individuals. DHS has taken interim measures to mitigate these concerns by developing two special clauses, Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015). These interim measures are necessary to ensure the protection of sensitive information while DHS completes the formal rulemaking process to include the new contractual language in the Homeland Security Acquisition Regulation. The special clauses strengthen the security of contractor IT systems and define contractor responsibilities when responding to a sensitive information incident. The applicability of the special clauses is limited to existing and new contracts and solicitations that have a **high risk** of unauthorized access to or disclosure of sensitive information.

3. Applicability of DHS Special Clauses:

(a) **Safeguarding of Sensitive Information (MAR 2015)** (See Attachment 1): Contracting officers shall incorporate this special clause or a subset[1] of the special clause language into existing and new high risk contracts and solicitations where (1) a contractor will have/has access to sensitive information, as defined in HSAR 3052.204-71 Contractor Employee Access, or (2) contractor IT systems are used to input, store, process, output, and/or transmit sensitive information. The Program Manager (PM), in close coordination with the Headquarters or Component Head of Contracting Activity (HCA), Chief Information Officer (CIO), Chief Security Officer (CSO), and Privacy Officer, will determine whether the existing contract, existing solicitation or new solicitation poses a high risk for unauthorized access to or disclosure of sensitive information. The ultimate decision to incorporate the special clause or a subset of the clause language into a solicitation or contract rests with the HCA. Contracting officers shall incorporate the special clause as follows:

- For existing contracts determined to be high risk, contracting officers shall bilaterally negotiate this special clause or a subset of the clause language into existing contracts.

- For existing solicitations determined to be high risk, contracting officers shall amend the solicitation to include this special clause and ensure the special clause is included in the resultant contract.

- For new solicitations determined to be high risk, contracting officers shall include this special clause in the solicitation and resultant contract.

- For existing contracts, existing solicitations and new solicitations, contracting officers shall also include HSAR clause 3052.204-71, Contractor Employee Access, and in coordination with legal counsel, consider whether inclusion of FAR clause 52.227-17 Rights in Data -- Special Works is appropriate if data includes personally identifiable information (PII), Sensitive PII, Sensitive Security Information (SS1), or any other Sensitive Information where there is a specific need to limit the contractor's distribution or use of the data.

(b) **Information Technology Security and Privacy Training (MAR 2015)** (See Attachment 2): Contracting officers shall incorporate this special clause into existing and new high risk contracts and solicitations where (1) a contractor will have/has access to sensitive information, as defined in HSAR 3052.204-71 Contractor Employee Access, or (2) contractor IT systems are used to input, store, process, output, and/or transmit sensitive information. The PM, in close coordination with the Headquarters or Component HCA, CIO, CSO, and Privacy Officer, will determine whether the existing

[1] A subset of the special clause language would be appropriate in instances such as, (1) a provision in the special clause is duplicative based on current contract terms and conditions, (2) the risk analysis provided by the Program Manager determined that it is not appropriate to include all of the requirements identified in the new special clause, (3) there is not enough time remaining in the period of performance to fulfill all of the clause requirements, etc.

contract, existing solicitation or new solicitation poses a high risk for unauthorized access to or disclosure of sensitive information. The ultimate decision to incorporate the special clause into a solicitation or contract rests with the HCA. Contracting officers shall incorporate the special clause as follows:

- For existing contracts determined to be high risk, contracting officers shall bilaterally negotiate this special clause into existing contracts.

- For existing solicitations determined to be high risk, contracting officers shall amend the solicitation to include this special clause and ensure the special clause is included in the resultant contract.

- For new solicitations determined to be high risk, contracting officers shall include this special clause in the solicitation and resultant contract.

4. Applicability of HSAR clauses 3052.204-70 and 3052.204-71:

The applicability of HSAR clause 3052.204-70 has been expanded from solicitations that require submission of an IT Security Plan to solicitations and contracts where contractor IT systems are used to input, store, process, output, and/or transmit sensitive information. The applicability of HSAR clause 3052.204-71 has been expanded from solicitations and contracts where contractor employees require recurring access to Government facilities or access to sensitive information to include solicitations and contracts where contractor IT systems are used to input, store, process, output, and/or transmit sensitive information. The prescription for HSAR clauses 3052.204-70 and 3052.204-71 is located at HSAR 3004.470-3, Contract clauses (Deviation), and has been revised to reflect the changes outlined below (See Attachment 3).

Effective immediately, Contracting Officers shall include:

a) HSAR clause 3052.204-70, in solicitations and contracts where contractor IT systems are used to input, store, process, output, and/or transmit sensitive information, but DHS special clause Safeguarding of Sensitive Information (MAR 2015) is not included; and

b) HSAR clause 3052.204-71 when issuing a solicitation or awarding a contract, where contractor employees require recurring access to Government facilities; contractor employees require access to sensitive information; or contractor IT systems are used to input, store, process, output, and/or transmit sensitive information. The prescription for the use of the alternates to HSAR 3052.204-71 is not changed by this class deviation.

5. Clause Applicability Matrix:

The following matrix illustrates the new applicability requirements of these clauses:

Clause Applicability Matrix		
Clause	**Use…**	**Do not use…**
HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources (JUN 2006)	In solicitations and contracts where contractor IT systems are used to input, store, process, output, and/or transmit sensitive information.	In solicitations and contracts where DHS special clause Safeguarding of Sensitive Information (MAR 2015) is in the solicitation or contract.
Safeguarding of Sensitive Information (MAR 2015)	In solicitations and contracts determined to be **high risk** where: ✓ a contractor will have access to sensitive information; or ✓ contractor IT systems are used to input, store, process, output, and/or transmit sensitive information.	In solicitations and contracts where HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources (JUN 2006) is in the solicitation or contract.
Information Technology Security and Privacy Training (MAR 2015)	When special clause Safeguarding of Sensitive Information (MAR 2015) is included in the solicitation or contract.	In solicitations and contracts where HSAR 3052.204-70, Security Requirements for Unclassified Information Technology Resources (JUN 2006) is in the solicitation or contract.

NOTE: HSAR clause 3052.204-71 Contractor Employee Access shall always be included in solicitations and contracts where (1) contractor employees require recurring access to Government facilities; (2) contractor employees require access to sensitive information; or (3) contractor IT systems are used to input, store, process, output, and/or transmit sensitive information.

6. Requirements Traceability Matrix:

The PM shall, in close coordination with the Headquarters or Component CIO or designee, ensure the Requirements Traceability Matrix (RTM) is prepared when a contractor IT system will be used to input, store, process, output, and/or transmit sensitive information. The RTM is generated based on the results from completing the FIPS 199 Categorization Workbook and E-Authentication Workbook. The RTM identifies the security controls that must be implemented on the contractor's IT system and is necessary for the contractor to prepare a Security Authorization package. PMs are reminded that the minimum rating for the "Confidentiality" and "Integrity" security objectives shall be no less than "Moderate" when an IT system will be used to input, store, process, output, and/or transmit PII, SPII, or SSI. Contracting officers shall include the RTM in new high risk solicitations and contracts when a contractor IT system will be used to input, store, process, output, and/or transmit sensitive information. Contracting officers shall also amend existing high risk solicitations to include the RTM and bilaterally negotiate the RTM into existing high risk contracts as needed.

7. Expiration Date:

This class deviation is applicable until the HSAR is changed by publication in the Code of Federal Regulations.

8. Additional Information:

Questions regarding this class deviation should be directed to Shaundra Duggans, Shaundra.Duggans@hq.dhs.gov, (202) 447-0056.

9. Attachments:

This class deviation is applicable until the HSAR is changed by publication in the Code of Federal Regulations.

- Attachment 1: Special Clause - Safeguarding of Sensitive Information (MAR 2015)
- Attachment 2: Special Clause - Information Technology Security and Privacy Training (MAR 2015)
- Attachment 3: HSAR 3004.470-3 Contract clauses. (Deviation)

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

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

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

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

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

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

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

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

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

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

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(f) *Sensitive Information Incident Reporting Requirements.*

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

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

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

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

(g) *Sensitive Information Incident Response Requirements.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(End of clause)

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

(b) *Security Training Requirements*.

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

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

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

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

(End of clause)

HSAR 3004.470-3 Contract clauses. (Deviation)

(a) Contracting officers shall insert a clause substantially the same as the clause at (HSAR) 48 CFR 3052.204-70, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts where contractor IT systems are used to input, store, process, output, and/or transmit sensitive information. However, when special clause Safeguarding of Sensitive Information (MAR 2015) is in the solicitation or contract (HSAR) 48 CFR 3052.204-70, Security Requirements for Unclassified Information Technology Resources shall not be used.

(b) Contracting officers shall insert the basic clause at (HSAR) 48 CFR 3052.204-71, Contractor Employee Access, in solicitations and contracts when contractor employees require recurring access to Government facilities; contractor employees require access to sensitive information; or contractor IT systems are used to input, store, process, output, and/or transmit sensitive information.

(1) Contracting officers shall insert the basic clause with its Alternate I for acquisitions requiring contractor access to IT resources.

(2) For acquisitions in which the contractor will not have access to IT resources, but the Department has determined contractor employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, the contracting officer shall insert the clause with its Alternate II.

(3) Neither the basic clause nor its alternates shall be used unless contractor employees will require recurring access to Government facilities or access to sensitive information and/or contractor information technology systems are used to input, store, process, output, and/or transmit sensitive information. Neither the basic clause nor its alternates should ordinarily be used in contracts with educational institutions.

(c) Contracting officers shall insert special clause Information Technology Security and Privacy Training (MAR 2015) in solicitations and contracts that contain special clause Safeguarding of Sensitive Information (MAR 2015).