FACT-FINDING SERVICES

STATEMENT OF WORK

MAY 2020

1 BACKGROUND

The mission of DHS, Office for Civil Rights and Civil Liberties (CRCL), Anti-Harassment Unit (AHU) is to enforce the DHS Anti-Harassment Policy. The DHS Anti-Harassment Policy prohibits harassment by any DHS employee, or harassment of any DHS employee, by any employee, contractor, vendor, applicant, or other individual with who DHS employees come into contact by virtue of their work for DHS. The Policy also prohibits harassing conduct that has a direct nexus to an individual's position or responsibilities regardless of whether it occurs on-duty, off-duty, face-to-face, via electronic means (e.g., telephone, email, social media, chat applications, etc.), through a third party, or through other means. Specifically, CRCL/AHU conducts inquiries into allegations of harassment brought by DHS-HQ employees that may be a violation of the DHS Anti-Harassment Policy.

The Department of Homeland Security (DHS) Headquarters Anti-Harassment Unit reports directly to CRCL's Deputy Officer for EEO and Diversity, and is responsible for overall management, administration, and oversight of the DHS-HQ AHU program.

1.1 References

The following references are pertinent to the work to be performed for this requirement:

- DHS Policy Statement, 256-06
- DHS Directive and Instruction 256-01
- EEOC's Management Directive-110
- Title VII of the Civil Rights Act of 1964 (Title VII), 42 U.S.C. §§ 2000(e) - 2000(e-17)
- Section 501 of the Rehabilitation Act of 1973 (Rehabilitation Act), 29 U.S.C. § 791.
- The Age Discrimination in Employment Act of 1967 (ADEA), 29 U.S.C. §§ 621-634 (2015)
- The Equal Pay Act of 1963 (EPA), 29 U.S.C. § 206 (d)(1)
- The Genetic Information Nondiscrimination Act of 2008 (GINA), 42 U.S.C. §§2000(ff)-2000(ff-11)

2 SCOPE

The purpose of this task order is to procure fact-finding support services for CRCL/DHS-HQ AHU. These services relate to reports of harassment brought to the DHS-HQ AHU by DHS-HQ employees. All services shall be performed in accordance with DHS Directive

REL0001333650

256-01, DHS Instruction 256-01 and the AHU Standard Operating Procedures.

3 TASK REQUIREMENTS

3.1 FACT FINDING SERVICES

The Contractor shall provide Fact-Finding services that include the following:

3.1.1 Develop an impartial and appropriate factual record upon which to make findings on claims raised by Complainants. An appropriate factual record is one that allows a reasonable fact finder to draw conclusion as to whether or not harassment occurred.

3.1.2 Arrange and conduct interviews with complainant(s), witnesses, and managers relative to the complainant. Draft official declarations based on interviews and obtain signature(s) of interviewees. DHS HQ AHU will provide boilerplate declaration form, fact-finding report template, and all other relevant templates used by the DHS-HQ AHU. Interviews shall be performed onsite at CRCL or at the worksite of the interviewee. For interviews that will be conducted at CRCL, the contractor will contact the AHU Director, or his/her designee, to schedule a conference room. Telephonic interviews are conducted upon approval of the Director of the AHU program.

3.1.3 Request and gather relevant documentation such as statistical, personnel data, and objective evidence (e.g., medical records that would verify injury or harm).

3.1.4 Secure testimony, which may be in the form of letters, interrogatories, taking on-site or telephonic sworn affidavits, preparing testimony of the complainant(s) and witnesses.

3.1.5 Secure approval from the AHU Director prior to expanding the scope of the investigation.

3.1.6 The estimated number of hours to complete an inquiry is 40 hours. If the contractor indicates that more than 40 hours is needed to complete the case, he/she shall notify the Anti-Harassment Director and the COR how many additional hours will be needed. The Contractor shall not continue work until the Director approves the additional hours.

3.1.7 The Contractor shall participate in section team meetings electronically or in person as scheduled by the DHS HQ Anti-Harassment Director.

REL0001333650

3.1.8 Contractors assigned to DHS cases must be US Citizens and able to secure the appropriate clearance.

3.2 SURGE SUPPORT

The Contractor shall have the capability to provide case support for Fact-Finding services as circumstances dictate. These additional services will be required as optional and only initiated if required post award. In order to meet this need, the Contractor shall maintain a pool of appropriately qualified resources. Services and deliverables shall be the same as those services outlined in paragraphs 4.1 and 4.2, and deliverable products identified in the Deliverable table.

3.4 REPORTING REQUIREMENTS

The Contractor shall provide the reports listed below, including all data and analysis created as part of this task order.

3.4.1 Complete Case File

The completed case file shall be provided to the CRCL Anti-Harassment Director upon submission of the final fact-finding report. A complete case file includes, all signed declarations, fact-finder notes and documents obtained during the course of the fact-finding.

3.4.1 Fact-Finding Reports

The Contractor shall provide a Fact-Finding Report, as outlined in Management Directive and Instruction 256-06 for each fact-finding performed. A draft report shall be provided via electronic media (in Microsoft Word 2016-compatible format), within 45 calendar days after assignment. Upon Government approval of the draft Report, the Contractor shall provide a Final Report, and the complete case file, within 5 calendar days. The contractor must also provide an itemized list of hours used.

4 CONTRACTOR PERSONNEL

4.1 Qualified Personnel

REL0001333650

The Contractor shall provide qualified personnel to perform all requirements specified in this task order.

4.1.1 All contract fact-finders shall possess the required training as outlined in Instruction 256-06. Additionally, investigators must have at least five years of investigative experience.

4.1.2 Contractor personnel must have excellent writing skills, superior factual and analytical ability, ability to work with minimal supervision, and professional objectivity. Experience could be gained as a federal employee, as a contractor supporting a federal agency, as an intern assigned to a federal agency, or in any other position requiring detailed knowledge and understanding of the theory of discrimination regarding harassment and 29 C.F.R. § 1614.101 *et seq.*

4.1.3 The Contractor shall ensure that contractor personnel remain abreast of statutory, regulatory, and case law development arising under relevant employment statutes by providing specialized training and/or technical assistance opportunities to contractor staff members at least annually through attendance at EEOC Training Institute presentations or similar instructional opportunities.

4.2 Project Manager

The Contractor shall provide a Project Manager (PM) who shall be responsible for all contractor work performed under this task order. The PM is further designated as *Key* by the Government.

The PM shall be a single point of contact for the Contracting Officer (CO) and the Contracting Officer's Representative (COR). It is anticipated that the PM shall be one of the senior level staff members provided by the Contractor for this work effort.

The name of PM, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the PM, shall be provided to the Government as part of the Contractor's proposal. During any absence of the PM, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this task order. The PM and all designated alternates shall be able to read, write, speak and understand English. Additionally, the Contractor shall not replace the PM without prior acknowledgement from the CO.

REL0001333650

The PM shall be available to the COR between the hours of 8:30 a.m. and 5:00 p.m. EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within two hours of notification.

The PM shall assign work to contractor staff members, monitor production (quantity), ensure quality of work, and serve as liaison between the COR, assigned CRCL POC, and contract personnel.

4.3 Key Personnel

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract:

- Project Manager

5 INTELLECTUAL PROPERTY

All Contractor-developed processes and procedures and other forms of intellectual property first developed under this task order shall be considered Government property.

All documentation, electronic data, and information collected by the Contractor and entered into a database or generated in support of this task order shall be considered Government property, and shall be returned to the Government at the end of the performance period.

REL0001333650

6 PROTECTION OF INFORMATION

Complaint files contain personal data that must be treated in a confidential manner. Contractor use is restricted to contractor personnel directly involved in preparing or reviewing the deliverables described in this statement of work. Material from complaint files transmitted electronically from the Contractor to the Government (as well as such transmissions between Contractor personnel) must first be encrypted and password protected, with password identification transmitted by separate communication, except that documents uploaded to a secure online portal do not require password protection.

Generally, the Government will not need to provide the Contractor with any printed materials from a complaint file, and the Contractor will not need to produce any printed materials from a complaint file. However, in the unusual case in which it is necessary for the contractor to possess printed material from a complaint file, such documents must be stored in a locked cabinet or secure area.

7 SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities, unless it would pose an undue burden to do so. Federal employees and members of the public who have disabilities must have access to and use of information and services that is comparable to the access and use available to non-disabled Federal employees and members of the public. For additional information, please refer to FAR 39.2 or http://www.section508.gov.

8 GOVERNMENT TERMS & DEFINITIONS.

a) DHS - Department of Homeland Security
b) CRCL - Office for Civil Rights and Civil Liberties
c) CO – Contracting Officer
d) COR – Contracting Officer's Representative
e) PM - Project Manager
f) Title VII - Title VII of the Civil Rights Act of 1964, as amended
g) ADEA - Age Discrimination in Employment Act

REL0001333650

h) ADA Amendments Act – ADA Amendments Act of 2008
i) GINA – Genetic Information Nondiscrimination Act of 2008
j) CFR - Code of Federal Regulations
k) EEO - Equal Employment Opportunity
l) EEOC - Equal Employment Opportunity Commission
m) 29 C.F.R. §1614.101 *et seq.* - Title 29, Code of Federal Regulations Part 1614
n) EEOC Management Directive 110 (MD-110)

DELIVERIES AND PERFORMANCE

1 PERIOD OF PERFORMANCE

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

2 PLACE OF PERFORMANCE

The place of performance for work performed under this task order will be at the Contractor's site in addition to the CRCL Office at Department of Homeland Security 2707 Martin Luther King Jr AVE SE Washington, DC 20528 and any other future CRCL Office.

3. Travel

The Contractor may be required to travel to support this contract. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. Reimbursement of local travel and commuting expenses is not authorized. Time-in-travel costs are not reimbursable. The Contractor shall be responsible for obtaining the Contracting Officer's Representative (COR) approval (electronic e-mail is acceptable) for all reimbursable travel in advance of each travel event. The Contractor shall also submit by email within 30 days to both the COR and the DHS Invoicing Team an invoice for work and travel performed. The invoice shall include required information outlined in the contract. Failure to submit a timely invoice may result in reimbursement and payment delays.

REL0001333650

3 GOVERNMENT-FURNISHED RESOURCES

The Government shall provide contractor personnel with the applicable documents, electronically in most cases, pertaining to the complaint file. For EEO counseling services, these documents will include any intake documents. For EEO investigative services, these documents will include intake documents, the Counselor's Report, the formal complaint, the acknowledgment letter, the acceptance letter, and a letter of authority.

4 GOVERNMENT FURNISHED PROPERTY

The Government shall provide equipment to include DHS laptops and/or DHS cell phones. Contractors shall obtain DHS PIV cards in order to access the DHS Laptops and to gain access to the CRCL office and CRCL facilities.

5 CONTRACTOR FURNISHED PROPERTY

The Contractor shall **not** furnish all facilities, supplies, materials, equipment, and services necessary to fulfill the requirements of this task order.,The Government will provide the supplies, materials and equipment, to include laptop and cellphone, to fulfill the requirements of this task order.
deliverables and delivery schedule
The Contractor shall ensure that the 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 electronic version only, using MS Office or Adobe applications, unless the COR requests a printed copy in a particular case. Daily, weekly, and interim information deliverables and working-copy products may be provided by email, as arranged with the COR.

The Government will have ten (10) business days to accept or reject task order 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.

REL0001333650

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

6.1 Deliverables

The Contractor shall provide the deliverables identified in the table below in electronic format only, via a secure online portal, unless the COR requests a printed copy in a particular case. Electronic copies shall be delivered via a secure online portal, or by other means by mutual agreement of the parties. All electronic deliverables shall be prepared using Microsoft or Adobe applications in formats selected by the Contractor. All deliverables shall be provided in accessible (Section 508 compliant) format, with read/write capability using applications that are compatible with Microsoft Office 2016 applications and Adobe Acrobat X, and delivered via secure online portal. Notification should be provided to the Assigned CRCL POC when a new document has been uploaded to the portal. The Contractor's deliverables shall not contain any identifiable corporate markings.

Item	RFQ Reference	Deliverable/Event	Due Date	Distribution
1		Post Award Conference	Within five (5) Business Days of Task Order Award or as coordinated by the CO/CS	In person meeting or by conference call
2		Kick Off Meeting	Within five Business Days of Task Order Award or as coordinated by the COR	In person meeting or by conference call
3		Draft Contractor Project Plan	Presented at Kick-Off meeting	COR, CO
4		Final Contractor Project Plan	Five business days after Kick-Off meeting	COR, CO
5		Progress Reports	4:00 PM EST every Monday beginning two weeks after date of award	COR, Assigned CRCL POC
6		Ad-Hoc Reports	As Requested by the COR	COR
7		Draft Fact-Finding Reports	45 calendar days after assigned by Director AHU	COR, Assigned CRCL POC
8		Final Fact-Finding Repors	5 calendar days after Government approval of Draft Fact-Finding Report	COR, Assigned CRCL POC

REL0001333650

9		Complete Case File	At the time submitting draft fact-finding report and complete case file	

6 GOVERNMENT ACCEPTANCE PERIOD

For Draft Deliverables, the Government will provide written comments and/or changes, if any, within the business days noted above, starting on the next business day after receipt by the Government of each Draft deliverable. Upon receipt of the Government comments, and unless otherwise noted above, the Contractor shall have five business days to incorporate the government's comments and/or change requests and to resubmit the deliverable in its final form. All of the Government's comments on deliverables must be incorporated in the succeeding version or the Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

For Final Deliverables, the Government will provide written notification of acceptance or rejection of all final deliverables provide written notification of acceptance or rejection within seven (7) business days counting from the next business of receipt. All notifications of rejection will include an explanation of the specific deficiencies causing the rejection.

If the Government finds that a final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements defined within the defined acceptance criteria, the document will be immediately rejected without further review and returned to the Contractor for correction and re-submission. If Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the COR which will include the CRCL POCs.

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

REL0001333650

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

REL0001333650

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,

REL0001333650

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.

REL0001333650

"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

REL0001333650

(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.

REL0001333650

(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.

REL0001333650

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

REL0001333650

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.

REL0001333650

(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

REL0001333650

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.

REL0001333650

(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

REL0001333650

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;

REL0001333650

(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)

REL0001333650