Federal Emergency Management Agency
Office of Equal Rights

FEMA

Performance Work Statement (PWS)
Organizational Health Assessment and Internal Climate and Culture Transformation Support Services

09/17/2022

REL0001297095

I. BACKGROUND

The Office of Equal Rights (OER) works to ensure that FEMA continues to meet its ongoing commitment to equal opportunity for its employees, applicants for employment at FEMA, and members of the public seeking access to FEMA programs and activities. OER's mission is to lead FEMA's efforts to promote fairness, integrity, compassion, and respect. OER holds themselves and the entire FEMA community accountable for doing the right thing. OER is committed to inspiring equality and inclusive diversity every day.

On June 25, 2021, Executive Order (EO) 14035 was disseminated to address strengthening the federal government's ability to recruit, hire, develop, promote, and retain our nation's talent and remove barriers to equal opportunity. In addition to providing resources and opportunities to strengthen and advance diversity, equity, inclusion, and accessibility across the federal government.

II. OBJECTIVE

The purpose of this Performance Work Statement (PWS) is to procure expert contractor services to provide change management support with the goal of reforming FEMA's climate and culture.

III. SCOPE

FEMA, OER requires Organizational Health Assessments (OHA) and Internal Climate and Culture Transformation Support Services. The scope of this requirement involves conducting Diversity, Equity, Inclusion, and Accessibility (DEIA) assessments. More specifically, developing OHA engagement strategies, performing research activities on the evolution of DEIA within FEMA's workforce, conducting analyses on research findings, developing, and presenting recommendations, and developing and implementing communication plans and change management support.

IV. SPECIFIC REQUIREMENTS

Task 1: Provide Project Management Support

The Contractor shall:

i. Track the project tasks of FEMA committees and ad-hoc groups, participate in meetings, communicate task progress with FEMA, and provide status reports.

ii. Support project onboarding and close-out activities.

iii. Conduct in-progress reviews as needed, including oral and written summaries of the project schedule and performance status.

REL0001297095

Task 2: Provide Administrative/Analytical Support

The Contractor shall:

i. Support gathering, interpreting, and/or utilizing data to develop actionable steps that will improve current processes and optimize results.

ii. Assess data to identify problems related to business operations and help to develop solutions to improve communication and/or data management.

iii. Conduct in-progress reviews as needed, including oral and written summaries of data findings.

iv. Provide recommendations for new business strategies or operational processes.

Task 3: Data Collection

The Contractor shall:

i. Assess historical data and current programs to identify actions to advance diversity, equity, inclusion, and accessibility in the workforce and remove any potential barriers to diversity, equity, inclusion, and accessibility in the workforce.

ii. Quantify demographic representation and trends related to diversity in the agency's workforce composition. Evaluations should include the following:

    a. Senior workforce composition
    b. Employment application
    c. Hiring decisions
    d. Promotions
    e. Pay and compensation
    f. Professional development programs
    g. Attrition rates

iii. Compile data charts and descriptive reports to evaluate fluctuating diversity trends in the agency's workforce composition from 2020 to present.

Task 4: Strategic Planning & Implementation

The Contractor shall:

i. Support the agency with developing quarterly goals and actions to advance diversity, equity, inclusion, and accessibility initiatives in the agency workforce and workplace culture.

REL0001297095

ii. Assist FEMA with gathering and compiling the annual progress report on the status of FEMA's efforts to advance diversity, equity, inclusion, and accessibility within the agency, and FEMA's success in implementing the Agency DEIA Strategic Plan.

Task 5: Training Development & Implementation

The Contractor shall:

i. Assist OER personnel with developing training programs that enable employees, managers, and leaders to develop knowledge in:
   a. Systemic and institutional racism and bias against underserved communities
   b. Building skillsets to promote respectful and inclusive workplaces and eliminate workplace harassment
   c. Acquiring knowledge of agency accessibility practices
   d. Increasing personnel understanding of implicit and unconscious bias
   e. Implementing equity-centered design across the agency

ii. Develop training programs and materials consistent with the goals for addressing cultural issues at FEMA. Training programs may include online, video, or in-person formats, handouts, wallet cards, presentations, interactive exercises, and other training aids.

iii. Develop and execute pulse surveys to incorporate real-time feedback on the program performance and pinpoint where course corrections may be required as well as document where new mindsets are taking hold, creating opportunities to celebrate successes and revisit approaches to rewards and recognition.

iv. Provide coaching and training for FEMA committees and ad-hoc groups to enable them to deliver consistent and appropriate messaging to employees in all FEMA components.

v. Develop an evaluation plan to measure the impact of the proposed program that includes providing recommendations to evaluate the proposed communication efforts and identify the type of data sets required to support FEMA's efforts to address its culture and realize improvements.

Task 6: Provide Communications Support Services

i. Develop a communications framework of key messages that will acknowledge FEMA's acceptance of its responsibility for the situation, stress FEMA's commitment to addressing deficiencies, and communicate plans, progress, and accomplishments as the culture is addressed and improvements are realized.

REL0001297095

ii. Create a comprehensive, integrated communications plan that identifies messages, themes, audience segments, new and existing communications media to be employed, timelines, and roles and responsibilities in order to provide awareness throughout the FEMA workforce and among selected outside audiences of efforts to bridge culture, policy, and procedure gaps and create a positive, productive, and inclusive work environment in all FEMA components.

iii. Provide creative design and development services to create print, digital, and video materials that can be used by FEMA to implement communications strategies developed under the communications plan. Provide creative services including e-mails, intranet pages or microsites, videos, posters, newsletters, mobile apps, presentations, podcasts, communications for FEMA TV, and displays.

iv. Provide consultative support, as requested, on issues pertaining to strategic communications and crisis communications, and facilitate internal meetings and discussion sessions to address new or unforeseen challenges that arise during the engagement to include, but not limited to, adverse events, changes in policies, changes in leadership, unfavorable news stories, or similar situations.

Task 7: Implementing Recommendations

i. Schedule and support an implementation kickoff meeting to initiate the project.

ii. Codify the recommendations in a change management communications plan.

iii. Determine success metrics for ensuring FEMA's goals are being met.

iv. Prepare an implementation action plan for implementing the recommendations for consideration by FEMA leadership.

v. Commence design and development efforts to support the implementation plan.

vi. Incorporate feedback to measure and monitor ongoing progress.

vii. Determine the frequency of results reporting and criteria for course corrections.

V. PERFORMANCE REQUIREMENTS SUMMARY

The table below specifies performance metrics with corresponding performance standards, surveillance methods, and incentives. These metrics apply to all work performed within each of the work areas. The Contracting Officer's Representative (COR) will document high quality performance and ensure it becomes part of the Contractor's past performance record, which will be entered at least annually into CPARS.

REL0001297095

Desired Output	Performance Standard	Acceptable Quality Level (AQL)	Monitoring Method	Incentive Schedule
Deliverables submitted on time	PWS required deliverables submitted on or before due dates without reminders from the PMO.	95%	PMO technical leads monitor due dates and notes when deliverables are submitted/ completed.	**Incentive:** COR will document high quality/high performance and ensure it becomes part of Contractor's past performance record which will be entered at least annually into CPARS. **Disincentive:** COR will document low quality/poor performance and ensure it becomes part of Contractor's past performance record which will be entered at least annually into CPARS
High quality deliverables	Deliverables submitted that meet or exceed requirements and support objectives of PWS. Deliverables do not include numerous spelling and grammatical mistakes or require significant re-work before being accepted by the Government.	95%	Designated lead, technical leads, COR, and/or CO review submitted deliverables and measure quality against standards in PWS and awarded contract as appropriate.	
Organized and productive meeting facilitation	Meetings are properly coordinated. Planning incorporates necessary meeting materials to include an agenda articulating a purpose and outcome(s) published in advance of the meeting. Meeting time is well managed, and the purpose and outcome(s) are achieved.	95%	Designated PMO lead monitors Contractor performance. PMO employees provide performance feedback to the COR and/or CO regarding meeting experience.	
Effective, clear, and concise status reporting	On a monthly basis the Contractor provides the designated PMO representative with a written review of contract performance to communicate task	95%	PMO technical lead, COR, and/or CO reviews provided information from the	

REL0001297095

	achievements, progress to date, and identified performance risks.		monthly report and ensures successful delivery of all required information.	

VI. PERIOD OF PERFORMANCE:

The period of performance shall be for one (1) base year of 12 months and four (4) 12-month option years. The period of performance reads as follows:

- Base Year
- Option Year I
- Option Year II
- Option Year III
- Option Year IV

VII. DELIVERABLES AND DELIVERY SCHEDULE:

Requirement	Deliverable	Method of Surveillance
Kick-off Meeting	The Contractor shall participate in a kick-off meeting with the Government no later than 10 business days after contract award. The contractor shall provide key personnel with authority to make decisions and take responsibility of any actionable items as a result of the meeting. The purpose of the meeting is to ensure that the contractor and Government understands the requirements outlined in the PWS. In addition to reviewing contract goals and objectives and to discuss technical requirements; administrative matters; security requirements; project transition; government furnished information, materials, and equipment; milestone schedule; review cycles; and invoicing.	100% Inspection – COR will review product for completeness & accuracy.
Project Management Plan (PMP)	Within 15 business days following contract award, the Contractor shall provide a comprehensive PMP detailing each task and deliverable. The PMP shall serve as a road map for executing each task, identifying contract requirements, outlining, and establishing communication processes, detailing roles and responsibilities, establishing sub-tasks and deliverables, and providing a detailed cost summary for each task. The PMP shall include a schedule	100% Inspection – COR will review product for completeness & accuracy.

REL0001297095

	for monthly financial reporting and required project status reporting.	
Monthly Status Reports (MSRs)	The Contractor shall provide MSRs by the 15th calendar day of every month. This report shall analyze the current tasks and include the following elements: • A summary of work performed and significant events by task functional area for the reporting period • Milestones and updates against task activities • Progress toward open efforts • New work started during the reporting period • Deliverables submitted or status on deliverable products in progress • Brief summary of goals and activities planned for the next reporting period • Problem areas, issues, or task risks requiring resolution, along with proposed corrective actions	100% Inspection – COR will review product for completeness & accuracy.
Draft & Final Reports	The Contractor shall provide draft, periodic, and final reports on projects related to the scoped tasks within the PWS. The Contractor shall be informed of report due dates by the program office for each new project. The final report shall encompass the work performed from the start to the end of the project. The draft and periodic reports shall analyze the current tasks and summary of work performed and projected work to be completed. Milestones and observed obstacles shall be outlined. Additional report content shall be defined by the program office, committee, and/or ad-hoc FEMA group.	100% Inspection – COR & Program/Project Lead will review product for completeness & accuracy.

The Government has 15 business days to review the deliverable and request edits, if needed, from the Contractor. The Contractor shall then have 15 business days to make the necessary revisions and resubmit the deliverable. The revised deliverable shall be reviewed and discussed prior to acceptance by the Government. If the Contractor does not receive comments from the Government by the stated deadline, acceptance can be assumed. Unless specified otherwise, deliverables may be delivered in electronic format using Microsoft products.

VIII. STATUS REPORTING

The Contractor shall convene with the COR monthly to report and discuss progress on tasks, budget, schedule, and other issues and items that may affect the successful completion of the task.

REL0001297095

IX. PLACE OF PERFORMANCE

The primary place of performance shall be at the DHS FEMA facility located at 500 C Street SW, Washington, DC.

The Contractor may be requested to work at other DHS FEMA facilities in the Washington Metropolitan area or from their designated Contractor facility.

Alternate places of performance shall be approved by the Contracting Officer.

X. TRAVEL

Contractor travel may be required to support this requirement. 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. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

XI. GOVERNMENT FURNISHED RESOURCES

The Government will furnish up to five (5) FEMA laptops for official Government business.

The Government will furnish existing FEMA OER policies.

XII. KEY PERSONNEL

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

Note: The Government may designate additional Contractor personnel as Key at the time of award.

The following Contractor personnel are designated as Key for this requirement:

- **Senior Program Manager (1)**

  Responsibilities: Plans complex and multifaceted projects in order to ensure completion to high standards of quality within timeframe and budget. Manages project teams. Creates specifications, budgets, work plans, timelines, and resource allocation models for projects. Leads the development of concepts, content, site maps, strategic plans, campaigns, and other production elements. Interfaces with clients for

REL0001297095

creative proposals and liaison meetings. Manages project budgets and financial reporting.

Qualifications: Requires 7+ years of experience as project manager. Requires fluency with the processes, language, and technology of creative production, along with superior organizational skills and superior attention to detail.

- **Program Manager (2)**

  Responsibilities: Plans projects of moderate complexity in order to ensure completion to high standards of quality within time frame and budget. Manages teams. Creates specifications, budgets, work plans, timelines, and resource allocation models for projects. Participates in the development of concepts, content, sitemaps, strategic plans, campaigns, and other elements. Interfaces with clients for creative proposals and liaison meetings. Manages project budgets and financial reporting.

  Qualifications: Requires 3-6 years of experience as project manager. Requires fluency with the processes along with superior organizational skills and attention to detail.

- **Data Analyst (1)**

  Responsibilities:
  - Identifying, analyzing, and interpreting fluctuating diversity trends in the agency's workforce composition from 2020 to present.
  - Evaluate and interpret historical data and trends or patterns in complex data sets.
  - Interfaces with clients to acquire programmatic data and liaison meetings.
  - Generate written reports to summarize data findings.

  Qualifications: Requires 3 - 5 years of experience as a data analyst, analyzing data using statistical techniques and producing reports. Requires proficiency in Microsoft Excel, fluency with the evaluating data and interpreting findings into a written report, superior organizational skills, and attention to detail.

- **Trainer (1)**

  Responsibilities:
  - Coordinate with OER's Training Lead to either assist or lead trainings related to, but not limited to, systemic and institutional racism and bias against underserved communities; building skillsets to promote respectful and inclusive workplaces and eliminate workplace harassment; personnel's understanding of implicit and unconscious bias; how to implement equity-centered design across the agency; and spreading knowledge of agency accessibility practices.
  - Collaborate with OER's Training Lead to develop necessary course materials, job aides, and acquiring course approval, as needed.

REL0001297095

- In collaboration with OER's Training Lead, provide training where necessary. These trainings range from formal classroom offerings to informal on-the-job training, as well as one-on-one coaching for FEMA staff.
- Provide recommendations to OER Training Lead and respective committees/ad-hoc groups on ways to improve training administration and materials.
- Develop surveys to gauge the effective of trainings.

Qualifications: Requires 3-5 years of experience as a trainer with experience administering courses related to diversity, equity, inclusion, and/or accessibility within federal education and training programs. Requires quality presentation skills, good writing skills, superior organizational skills, and attention to detail.

XIII. EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level, and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and always display all identification and visitor badges in plain view above the waist.

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and always display the Government issued badge in plain view above the waist.

XIV. EMPLOYEE CONDUCT

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

XV. REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will

REL0001297095

provide the Contractor with a written explanation to support any request to remove an employee.

XVI. CONTRACT TYPE

Firm-Fixed-Price (FFP) basis.

XVII. RECORDS MANAGEMENT OBLIGATIONS

A. *Applicability*

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. *Definitions*

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. includes FEMA records.
2. does not include personal materials.
3. applies to records created, received, or maintained by Contractors pursuant to their FEMA contract.
4. may include deliverables and documentation associated with deliverables.

C. *Requirements*

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.
2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5

REL0001297095

U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.
4. FEMA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of FEMA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to FEMA. The agency must report promptly to NARA in accordance with 36 CFR 1230.
5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the [contract vehicle]. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to FEMA control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the PWS. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).
6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and FEMA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.
7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with FEMA policy.
8. The Contractor shall not create or maintain any records containing any non-public FEMA information that are not specifically tied to or authorized by the contract.
9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

REL0001297095

10. The FEMA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which FEMA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.
11. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take FEMA-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

XVIII. SECURITY REQUIREMENTS

All personnel require access to information up to the sensitive but unclassified, for official use only (FOUO) levels. Contractor must ensure contractor employees receive a favorably adjudicated public trust suitability prior to entry on duty (EOD). All individuals will be U.S. citizens. The contractor shall follow the standards established within DHS and FEMA policy.

Unauthorized Disclosure of Classified or Unclassified Information:

Contractors and Subcontractors who are working on this contract shall receive Unauthorized Disclosure of Classified or Unclassified Information training.

Access to the training can be obtained at:

https://securityawareness.usalearning.gov/unauthorizedrefresher/index.htm

Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

OPSEC Training:

Contractors and Subcontractors who are working on this contract shall receive the OPSEC Awareness Brief.

Access to the briefing can be obtained at http://cdsetrain.dtic.mil/opsec

Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

REL0001297095

Insider Threat Training:

Insider Threat training for Contractors can be found at:
http://cdsetrain.dtic.mil/itawareness/index.htm.

Certificate of training is required for all cleared contractor employees who are working with classified or unclassified information. All certificates must be sent to the assigned FEMA Contracting Officer Representative, before the Contractor or Subcontractor is granted access to classified or unclassified information but no later than 30 calendar days after awarded contract. All cleared contractor personnel are required to recertify Insider Threat training annually thereafter. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

For Official Use Only (FOUO) Information:

In accordance with DHS Management Directive 11042.1 contractors, consultants and others to whom access is granted will abide by 11042.1; DHS policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities.

The contractor will:

1. Be aware of and comply with the safeguarding requirements for "For Official Use Only" (FOUO) information as outlined in this directive.
2. Participate in formal classroom or computer-based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.
3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

Contractors and Consultants shall execute a DHS Form 11000-6, *Sensitive but Unclassified Information Non Disclosure Agreement* (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon date of the DHS Policy and not applied retroactively.

Foreign Travel and Government-Issued Equipment

Per DHS and FEMA IT policy, FEMA employees and contractors are not authorized to take government-issued equipment, including cell phones, computers, or tablets such as

REL0001297095

iPads, outside of the United States regardless of the reason for travel. If government-issued equipment is required for official foreign travel, FEMA government employees may request a temporary loaner device through the Mobility Service Center.Office of the Chief Information Officer, Service Center for the duration of their trip. FEMA contractors must contact their contracting officer's representative (COR) for further guidance.

If your device is detected as operating outside of the United States and its territories it will be disabled, and your information will be forwarded to the Office of Professional Responsibility for review.

Background Investigations

All contractor personnel who require access to DHS or FEMA information systems, routine access to DHS or FEMA facilities, or access to sensitive information, including but not limited to Personally Identifiable Information (PII), shall be subject to a full background investigation commensurate with the level of the risk associated with the job function or work being performed. FEMA's Personnel Security Division (PSD) will determine the risk designation for each contractor position by comparing the functions and duties of the position against those of a same or similar federal position, applying the same standard for evaluating the associated potential for impact on the integrity and efficiency of federal service.

Low Risk without Information System Access

Contractor personnel occupying positions or performing functions with a Low Risk designation and who do not require access to DHS or FEMA information systems may undergo a Tier 1 investigation with a credit check and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract. (also reference Facility Access).

Low Risk with Information System Access

Contractor personnel occupying positions or performing functions with a Low Risk designation and who require access to DHS or FEMA information systems shall undergo a Tier 2 Suitability Background Investigation (T2) and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

Moderate Risk

Contractor personnel occupying positions or performing functions with a Moderate Risk designation shall undergo a Tier 2 Suitability Background Investigation (T2) and must

REL0001297095

receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

High Risk

Contractor personnel occupying positions or performing functions with a High Risk designation shall undergo a Tier 4 Suitability Background Investigation (T4) and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract.

Background Investigation Process

To initiate the request to process contractor personnel, the Contractor shall provide the FEMA Contracting Officer's Representative (COR) with all required information and comply with all necessary instructions to complete Section II of the FEMA Form 121-3-1-6, "Contract Fitness/Security Screening Request." The FEMA COR shall ensure that all other applicable sections of the FEMA Form 121-3-1-6 are complete prior to submitting the form to FEMA PSD for processing. The Contractor shall also provide the FEMA COR with completed OF 306, "Declaration for Federal Employment," forms for all contractor personnel.

Contractor personnel who already have a favorably adjudicated background investigation, may be eligible to perform work under this contract without further processing by FEMA PSD if:

- the investigation was completed within the last five years,
- it meets or exceeds the minimum requirement for the position they will occupy or functions they will perform on this contract,
- the contractor personnel have not had a break in employment since the prior favorable adjudication, and,
- FEMA PSD has verified the investigation and confirmed that no new derogatory information has been disclosed which may require a reinvestigation.

FEMA PSD will notify the COR of the names of the contractor personnel eligible to work based on prior, favorable adjudication. The COR will, in turn, notify the Contractor of the names of the favorably adjudicated contractor personnel, at which time the favorably adjudicated contractor personnel will be eligible to begin work under this contract.

REL0001297095

For those contractor personnel who do not have an acceptable, prior, favorable adjudication or who otherwise require reinvestigation, FEMA PSD will issue an electronic notification via email directly to the contractor applicant/personnel that contains the following documents, which are incorporated into this contract by reference, along with a link to the Office of Personnel Management's (OPM) Electronic Questionnaires for Investigation Processing (e-QIP) system and instructions for submitting the necessary information:

- Standard Form 85P, "Questionnaire for Public Trust Positions"
- Optional Form 306, "Declaration for Federal Employment"
- SF 87, "Fingerprint Card" (2 copies)
- DHS Form 11000-6, "Non-Disclosure Agreement"
- DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

FEMA PSD will only accept complete packages consisting of all of the above document and Standard Form 85P, which must be completed electronically through the Office of Personnel Management's e-QIP system. The Contractor is responsible for ensuring that all contractor personnel timely and properly submit all required background information.

Once contractor personnel have properly submitted the complete package of all required background information, FEMA's Personnel Security Division, at its sole discretion, may grant contractor personnel temporary eligibility to perform work under this contract prior to completion of the full background investigation if the Personnel Security Division's initial review of the contractor personnel's background information reveals no issues of concern. In such cases, FEMA's Personnel Security Division will provide notice of such temporary eligibility to the COR who will then notify the Prime Contractor, at which time the identified contractor personnel will be temporarily eligible to begin work under this contract. Neither the Prime Contractor nor the contractor personnel has any right to such a grant of temporary eligibility. The grant of such temporary eligibility shall not be considered as assurance that the contactor personnel will remain eligible to perform work under this contract upon completion of and final adjudication of the full background investigation.

Upon favorable adjudication of the full background investigation, FEMA's Personnel Security Division will update the contractor personnel's security file and take no further action. In any instance where the final adjudication results in an unfavorable

REL0001297095

determination FEMA's Personnel Security Division will notify the contractor personnel directly, in writing, of the decision and will provide the COR with the name(s) of the contractor personnel whose adjudication was unfavorable. The COR will then forward that information to the Contractor. Contractor personnel who receive an unfavorable adjudication shall be ineligible to perform work under this contract. Unfavorable adjudications are final and not subject to review or appeal.

Continued Eligibility and Reinvestigation

Eligibility determinations based on a Low Risk T1, Moderate Risk T2S or High Risk T4 are valid for five years from the date that the investigation was completed and closed. Contractor personnel required to undergo a background investigation to perform work under this contract shall be ineligible to perform work under this contract upon the expiration the background investigation unless and until the contractor personnel have undergone a reinvestigation and FEMA's Personnel Security Division has renewed their eligibility to perform work under this contract.

Exclusion by Contracting Officer

The Contracting Officer, independent of FEMA's Personnel Security Division, may direct the Contractor be excluded from working on this contract. Any contractor found or deemed to be unfit or whose continued employment on the contract is deemed contrary to the public interest or inconsistent with the best interest of the agency may be removed.

FACILITY ACCESS

The Contractor shall comply with FEMA Directive 121-1 "FEMA Personal Identity Verification Guidance," FEMA Directive 121-3 "Facility Access," and FEMA Manual 121-3-1 "FEMA Credentialing Access Manual," to arrange for contractor personnel's access to FEMA facilities, which includes, but is not limited to, arrangements to obtain any necessary identity badges for contractor personnel.

Contractor personnel working within any FEMA facility who do not require access to DHS or FEMA IT systems and do not qualify for a PIV Card may be issued a Facility Access Card (FAC). FACs cannot exceed 180 days; all contractors requiring access greater than 180 days will need to qualify for and receive a PIV card before being allowed facility access beyond 180 days.

Contractor personnel shall not receive a FAC until they have submitted a SF 87, "Fingerprint Card," and an OF306, Declaration for Federal Employment, and receive approval from FEMA PSD. Contractor personnel using a FAC for access to FEMA facilities must be escorted in Critical Infrastructure areas (i.e., server rooms, weapons rooms, mechanical rooms, etc.) at all times.

REL0001297095

FEMA may deny facility access to any contractor personnel whom FEMA's Office of the Chief Security Officer has determined to be a potential security threat.

SEPARATION FROM CONTRACT

The Contractor shall notify the FEMA COR of all terminations/resignations within five (5) calendar days of occurrence. The Contractor must account for all forms of Government-provided identification issued to contractor employees under a contract (i.e., the PIV cards or other similar badges) must return such identification to FEMA as soon as any of the following occurs:

- When no longer needed for contract performance.
- Upon completion of a contractor employee's employment.
- Upon contract completion or termination.

If an identification card or building pass is not available to be returned, the Contractor shall submit a report to the FEMA COR, referencing the pass or card number, name of the individual to whom it was issued, and the last known location and disposition of the pass or card.

The Contractor or contractor personnel's failure to return all DHS- or FEMA-issued identification cards and building passes upon expiration, upon the contractor personnel's removal from the contract, or upon demand by DHS or FEMA may subject the contractor personnel and the Contractor to civil and criminal liability.

FOR OFFICIAL USE ONLY

In accordance with DHS Management Directive 11042.1 contractors, consultants, and others to whom access is granted will abide by 11042.1; DHS policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities. The contractor will:

1. Be aware of and comply with the safeguarding requirements for "For Official Use Only" (FOUO) information as outlined in this directive.
2. Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.
3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

Contractors and Consultants shall:
Execute a DHS Form 11000-6, Sensitive but Unclassified Information Non Disclosure Agreement (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an N DA as determined by the applicable program

REL0001297095

manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

UNAUTHORIZED DISCLOSURE OF CLASSIFIED OR UNCLASSIFIED INFORMATION

Contractors and Subcontractors who are working on this contract shall receive Unauthorized Disclosure of Classified or Unclassified Information training.
Access to the training can be obtained at:
https://securityawareness.usalearning.gov/unauthorizedrefresher/index.htm
Send the certificate of completion to the FEMA Contracting Officer Representative no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

OPSEC TRAINING

Contractors and Subcontractors who are working on this contract shall receive the OPSEC Awareness Brief.
Access to the briefing can be obtained at http://cdsetrain.dtic.mil/opsec
Send the certificate of completion to the FEMA COR no later than 30 calendar days after awarded contract. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

INSIDER THREAT TRAINING

Insider Threat training for Contractors can be found at:
http://cdsetrain.dtic.mil/itawareness/index.htm.
Certificate of training is required for all cleared contractor employees who are working with classified or unclassified information. All certificates must be sent to the assigned FEMA Contracting Officer Representative, before the Contractor or Subcontractor is granted access to classified or unclassified information but no later than 30 calendar days after awarded contract. All cleared contractor personnel are required to recertify Insider Threat training annually thereafter. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

XIX. CYBER HYGIENE AND PRIVACY CLAUSES

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—

REL0001297095

"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);

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);

REL0001297095

(2) 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

(3) 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:

REL0001297095

(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.

REL0001297095

(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

REL0001297095

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.

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:

(i) 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

REL0001297095

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

REL0001297095

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;
(ii) (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(i) Government programs, platforms or systems involved;
(ii) Location(s) of incident;
(iii) Date and time the incident was discovered;
(iv) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;

REL0001297095

(v) Description of the Government PII and/or SPII contained within the system;
(vi) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(vii) 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

REL0001297095

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;

REL0001297095

(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.

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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.

Security Training Requirements.

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.

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

REL0001297095

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

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

REL0001297095