

Technical Support for Response and Recovery Missions

STATEMENT OF WORK (SOW)

A. PURPOSE and SCOPE

The primary mission of the Federal Emergency Management Agency (FEMA) is helping people before, during and after disasters. The range of FEMA's responsibilities is broad, far-reaching, and complex. FEMA's Office of Response and Recovery (ORR) provides guidance, leadership, and oversight to build, sustain, and improve the coordination and delivery of support to citizens and State, local, tribal, and territorial governments to save lives, reduce suffering, protect property, and recover from all hazards.

Additionally, ORR coordinates the Federal response and recovery capability needed to save and sustain lives, minimize suffering, and protect property in a timely and effective manner following natural disasters, acts of terrorism, or other emergencies. Operational activities include the coordination of all Federal emergency management response and recovery capabilities, and the integration of Federal, State, tribal and local disaster programs.

The purpose of this effort is to obtain technical support services for response and recovery missions under the Office of Response and Recovery (ORR) domain. Support will be provided to ORR including its directorates, regional offices, and field components. The scope includes (but is not limited to) the following areas:

- Training Development and Assessment

Necessary support personnel may include (but are not limited to) the following:

- Program Coordinator
- Facilitator Support
- Instructor/Training Specialist

B. PERIOD OF PERFORMANCE

Base period: From date of award to September 30, 2022.

Option Year 1: 11/01/2022-09/30/2023

Option Year 2: 10/01/2023-09/30/2024

Option Year 3: 10/01/2024-09/30/2025

Option Year 4: 10/01/2025-09/30/2026

C. PLACE OF PERFORMANCE

- Work could be conducted at any of the 10 Regional Offices, FIWA, HQ, Mt. Weather and/or additional identified locations within FEMA within the continental United States.
- Increasing from 12 (Twelve) FY deliveries to 18 (Eighteen) FY deliveries

FEMA Location	Address
FEMA Region 1	99 High St, 6th floor, Boston, MA 02110
FEMA Region 2	One World Trade Center, 285 Fulton Street, New York, NY 10007
FEMA Region 3	615 Chestnut St, Philadelphia, PA 19106
FEMA Region 4	3005 Chamblee Tucker Rd, Atlanta, GA 30341
Atlanta DC	3780 South Side Industrial Court, Atlanta, GA 30354
FEMA Region 5	536 South Clark St, 6th Floor, Chicago, IL 60605
FEMA Region 6	800 North Loop 288, Denton, TX 76209-3606
FEMA Region 7	11224 Holmes Road, Kansas City, MO 64131-3626
FEMA Region 8	555 17 th Street, Suite 1100 Denver, CO 80202
FEMA Region 9	1111 Broadway, Suite 1200, Oakland, CA 94607
FEMA Region 9 CRC West	10000 Goethe Rd. Suite B2, Sacramento, CA 95827
FEMA Region 10	130 228 th Street, Southwest, Bothell, WA 98021-9796

D. PERFORMANCE OBJECTIVES

I. Training Development and Assessment

The contractor shall

- In-Person deliveries may be staffed with a minimum of two (2) Unit instructors or Adjunct instructors. Support continuity of operations and devolution planning;
 - All contract instructors will provide documentation of completion of the Instructor Qualification Course (IQC) or equivalent.
 - Contractor shall comply with the National Integration Center's (NIC) ICS general instructor guidelines detailed on Page 8 – 9 of the ICS-300 POI and on Page 6 – 7 of the ICS-400 POI (see attachments). The contractor may request, and the government may facilitate, the contract instructor's attendance of the FIWA managed IQC and the EMI managed ICS-449 course if prerequisites are met and seats are available.
 - Contractor shall provide the COTR with a Biographical Summary of each instructor that includes the following information:
 - Whether the instructor will perform as a Unit or Adjunct instructor.
 - Instructor's relevant professional background.
- How the instructor's training and experience achieves NIC standards as detailed in the POI

- Provide qualified personnel;
1. Instructional Content: The instructional material will be provided by the government.
 - a. Contract instructors shall administer the training in a manner that is consistent with the most recent Plan of Instruction (POI); currently April 2019 Version 1.0 for ICS-300 and April 2019 Version 1.0 for ICS-400 (see attachments).
 - b. Adaptations to the POI are sometimes appropriate due to unanticipated changes, operational considerations, and to maximize efficiency. Requests for modification to the POI shall be coordinated through the Contracting Officers Technical Representative (COTR) and preapproved by the Course Manager at the Emergency Management Institute prior to implementation of changes to the POI.
 2. Minimum Staffing: In-Person deliveries may be staffed with a minimum of 2 Unit instructors or Adjunct instructors provided by the contractor.
 3. Instructor Qualifications:
 - a. All contract instructors will provide documentation of completion of the Instructor Qualification Course (IQC) or equivalent.

- b. Contractor shall comply with the National Integration Center's (NIC) ICS general instructor guidelines detailed on Page 8 – 9 of the ICS-300 POI and on Page 6 – 7 of the ICS-400 POI (see attachments). The contractor may request, and the government may facilitate, the contract instructor's attendance of the FIWA managed IQC and the EMI managed ICS-449 course if prerequisites are met and seats are available.
- c. Contractor shall provide the COTR with a Biographical Summary of each instructor that includes the following information:
 - Whether the instructor will perform as a Lead, Unit, or Adjunct instructor.
 - Instructor's relevant professional background.
 - How the instructor's training and experience achieves NIC standards as detailed in the POI.

4. Scheduling and Preparation:

- a. The government will provide the contractor a class schedule and student roster through DTS.
- b. The contractor shall ensure that all course material and in-person classrooms, are positioned for instructional delivery prior to the beginning of each class.
- c. The Contractor will be notified of any changes to the delivery schedule that may affect the delivery date or location at least 30 calendar days prior to the scheduled class date.
- d. Notice provided to the Contractor of changes to the schedule or location may be reduced from 30 days to 3 days upon the declaration of a Type I disaster.

E. PERFORMANCE STANDARDS OF SERVICES

The contractor shall:

- In-Person deliveries may be staffed with a minimum of 2 Unit instructors or Adjunct instructors provided by the contractor. Support continuity of operations and delegation planning.

Safeguarding of Sensitive Information (MAR 2015)

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

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

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

could be used to identify an individual.

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

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

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107- 296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee).
- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee).
- (3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest.
- (4) Any information that is designated “sensitive” or subject to other controls, safeguards, or protections in accordance with subsequently adopted homeland security information handling procedures.

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

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include Social Security numbers (SSN), driver’s license or state identification number, Alien

Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

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

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

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

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive but Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

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

- (1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term

“FOR OFFICIAL USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

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

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

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

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

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

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance

of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

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

Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a contractor IT system that will store, maintain, and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

(2) **Renewal of ATO.** Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods:

- (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or
- (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. Their views may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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

computer crime.

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

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

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

f. *Sensitive Information Incident Reporting Requirements.*

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

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting

requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

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

g. Sensitive Information Incident Response Requirements.

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

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

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

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

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

h. Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

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

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

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

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

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

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

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

- (i) A dedicated telephone number to contact customer service within a fixed period;
- (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
- (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be

handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

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

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 Clause)

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 31 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 31 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 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 31 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 31 of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of Clause)

Section 508 Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at <https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf>. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.
2. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.

3. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at <https://www.dhs.gov/508-testing>.
4. Contractor personnel shall possess the knowledge, skills, and abilities necessary to address the applicable revised Section 508 Standards for each ICT.
5. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018, and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018.

Instructions to Offerors

1. For each ICT Item that will be developed, modified, installed, configured, integrated, maintained, or hosted by the contractor pursuant to this contract, the offeror shall provide an acknowledgement of the Section 508 requirements and a detailed explanation of the Offerors plan to ensure conformance with the requirements. The Offeror shall also describe the evaluation methods that will be used to validate for conformance to the Section 508 Standards.

Acceptance Criteria

1. Before accepting items that contain Information and Communications Technology (ICT) that are developed, modified, or configured according to this contract, the government reserves the right to require the contractor to provide the following:
 - Accessibility test results based on the required test methods.
 - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
 - Documentation of core functions that cannot be accessed by persons with disabilities.
 - Documentation on how to configure and install the ICT Item to support accessibility.
 - Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).
2. Therefore, accepting ICT required under the contract, the government reserves the right to perform testing on required ICT items to validate the offeror's Section 508 conformance claims. If the government determines that Section 508 conformance claims provided by the offeror represents higher level of conformance than what is actually provided to the agency, the government shall, at its option, require the offeror to remediate the item to align with the offeror's original Section 508 conformance claims prior to acceptance.

Section 504 Requirements

The Contractor/Provider shall comply fully with Section 504 of the Rehabilitation Act of 1973, as amended, which prohibits discrimination against qualified individuals with disabilities. No otherwise qualified individual with a disability shall, solely by reason of his or her disability, be excluded from participation in, be denied the benefits of, or subjected to discrimination under any program or activity for which the Contractor/Provider is awarded a contract and/or receives federal financial assistance from the Federal

Emergency Management Agency. This includes, but is not limited to, providing reasonable accommodations and modifications to ensure effective communication access, physical access, and program access to all participants, including persons with disabilities. The Contractor/Provider shall incorporate this language in any subcontracts related to the provision of the FEMA public-facing program or activity.

SECURITY: 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.

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.

Unauthorized Disclosure of Classified or Unclassified Information

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