HMTAP 506

DTA Technical Assistance - Sector B

Statement of Objectives 02/21/2023

This section is completed by COR

Task Order Number	HMTAP 506 Direct Technical Assistance
Acquisition Planning Forecast System (AAP#)	NA
Document Control Number (from FEMA Form 40-1)	TBA
Competitive Task Order?	Yes __ No _X_
Contract Number	70FA6020D00000002 - Sector B
Task Order Funding Type	Choose an item. Please provide a justification if other than FFP Requirement involves multiple phases of grant application process and cannot be clearly defined. Resources fluctuate depending on the complexity of each grant project.
Contract Task	Technical Activity Technical Advisement
COR Notes	

This section is completed by the requesting office.

Task Order Title	HMTAP 506 - BRIC Direct Technical Assistance Sector B	
Period of Performance	12 months from award plus one option period	
Disaster Number *(if applicable)*	X	Not Applicable
Headquarters/Region	Sector B Regions	If other, specify:
Location of Work *(City and state where work will be completed)*	Sector B Regions	
Maximum pages allowed for Performance Work Statement (excluding resumes) *(Please select one)*	For Technical Approach & Staff Qualifications: 20 pages	
Need Individual Staff Qualifications? *	Yes	

** Resume(s) will be submitted for key personnel.*

PURPOSE

Provide a general background that illustrates the need for the project. Create a statement of purpose.

The purpose of this task order is to support the BRIC program in providing Direct Technical Assistance (DTA) to increase the capacity and capabilities of disadvantaged communities in Sector B - FEMA Region I (Connecticut, Maine, Massachusetts, Rhode Island, Vermont, New Hampshire), Region II (New Jersey, New York, Puerto Rico, Virgin Islands), Region III (District of Columbia, Maryland, Delaware, Pennsylvania, Virginia, West Virginia), and Region IV (Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee) through the FEMA Hazard Mitigation Assistance (HMA), Building Resilient Infrastructure and Communities (BRIC) Program.

Assistance will include support for mitigation projects, such as, virtual and in-person site visits; guidance; stakeholder and partner engagement; hazard risk assessment; mitigation project identification and conceptualization; mitigation planning; and development of Hazard Mitigation Assistance grant applications.

This will enable the FEMA HQ BRIC Program Office to expeditiously enable low-capacity communities to increase disaster resilience, improve mitigation outcomes, and foster capability and capacity building to reduce disaster suffering and costs, and address inequitable risks certain communities face. In most cases, this technical assistance will lead to future mitigation projects that can be implemented directly by tribal, state and local governments. The BRIC program is one of several federal programs within the pilot program

of the Justice40 Initiative. The Interim Implementation Guidance on the Justice40 Initiative can be found at "https://www.whitehouse.gov/wp-content/uploads/2021/07/M-21-28.pdf."

Information about non-financial Direct Technical Assistance is available at BRIC Direct Technical Assistance | FEMA.gov.

This work supports the FEMA and Federal Insurance and Mitigation Administration objectives and priorities for diversity, equity, and inclusion.

OBJECTIVES

List each objective you would like the contractor to achieve. Provide detail as necessary to guide the contractor on the parameters of each objective.

Overview of Objectives:

The Contractor will provide described services for an estimated twenty-five (25) communities that will be named not later than April 30, 2023, for the base year, and an estimated thirty-four (34) communities for the option year that will be named not later than April 20, 2024. FEMA will not know the potential project types until after award, but all will involve hazard mitigation.

The communities will be selected using the prioritizing criteria listed in the FY 22 FEMA BRIC Direct Technical Assistance Program Support Material found here: BRIC Direct Technical Assistance (fema.gov).

Each of the communities in the base year and option year will be allotted up to 600 hours per community over a one (1) year period for technical assistance, i.e., 15,000 hours in the base year and 20,400 hours in the option year; travel included. This will be a coordinated effort by FEMA staff and the Contractors. The contractor can expect to be engaged throughout the span of the allotted hours.

We estimate up to 50 five-day site visits (2 per community) for this task order may be conducted in the base year within designated Sector geographical area. This assistance may be provided in a virtual environment should conditions warrant.

We also estimate up to 68 five-day site visits will be needed for the option period (2 per community).
The total Period of Performance for this effort will not exceed 24 months, which includes one 12-month base period and one 12-month option period with all objectives being the same for each year.

The below objectives will apply to each of the communities serviced:

OBJECTIVE: 1 Task Order Administration: - Base Period

The Contractor shall provide project administration services to support and manage the activities associated with all the elements of the Statement of Objectives. These services and support include:

1. Coordinate a preliminary kickoff meeting within 5 business days of the Notice to Proceed (NTP) with the Contracting Officer Representative (COR), Project Monitor (PM) and Technical Monitor (TM) where the initial work plan shall be discussed.
2. Provide meeting minutes from the kickoff meeting within 2 business days of the meeting.
3. Provide a work plan to the COR and PM within 10 days of the kickoff meeting. The baseline work plan must include information on the process the Contractor shall utilize for QA/QC on this project.
4. Provide a Quality Control Plan within 10 days of the kickoff meeting. The QCP will be reviewed and approved by the PM and TM to ensure quality responses and minimize the number of responses requiring follow-ups to correct incomplete, erroneous, or otherwise insufficient information. The QCP may be submitted as a separate document or an attachment to the workplan.
5. Facilitate and compile written meeting minutes reflecting coordination and technical assistance meetings, held in person, via conference call or webinar, on at least a monthly basis for the duration of the task order.
6. In conjunction with the program office, the Contractor must use appropriate internet accessible means to manage and monitor the performance and progress of tasks. Tools may include items capable of web accessible document sharing, illustration, and tracking of project schedules. These tools are to be independent of and not directly integrated with any FEMA information system.
7. Provide status of tasks when determined necessary by the program office, which may be as frequent as weekly. Status must include hours and costs incurred by the prime contractor as well as any subcontractor, partner, or associate for each community served.
8. Provide monthly progress reports. The reports shall be prepared and submitted to the PM and COR.
9. All task deliverables and status/progress reports, as well as invoicing must be itemized by task and name of community that received the assistance.
10. Coordinate with two other HMTAP Sectors to ensure coordinated service delivery across the United States and its territories.

OBJECTIVE: 2 Provide technical support for Direct Technical Assistance (DTA) Communities – Base Period

The Contractor Shall be capable of interacting and collaborating with communities and other FEMA stakeholders in order to achieve the objects described below as necessary in providing technical assistance for the aforementioned 59 communities.

FEMA staff will do a preliminary assessment of each community and develop preliminary DTA workplans, which will be updated as progress occurs throughout the process.

The DTA workplans will be monitored by the contractor through check-ins with the community or tribe, FEMA Region, State Hazard Mitigation Officer (as applicable), and FEMA DTA Headquarters staff. This monitoring will be continuous throughout the contract to track community goals related to the Direct Technical Assistance. Estimated every 2 weeks for the first 3 months and monthly after that but will vary by community.

Not all the work listed below will be necessary at all locations. Some will be supported by FEMA staff. Coordination of Contractor support will depend on the timing of the execution of work with the individual communities. Tasking must be coordinated with FEMA Region Staff including FEMA Region BRIC DTA Point of Contact and/or FEMA Region Tribal Specialist.

The communities will work with the FEMA Region to coordinate the necessary technical assistance actions to be provided. Assistance will be a coordinated effort and could fall on either both the contractor and the region.

Tasks/objectives may include:

1. Perform field reconnaissance, benefit cost analysis, and hazard risk assessments, in order to identify, develop and/or review hazard mitigation project applications including climate and future conditions adaptation.
2. Conceptualize and explore opportunities for the development of BRIC grant applications.
3. Provide assistance with mitigation planning, and grants administration and support with stakeholder and partner engagement.
4. Identify and/or collect information, standards, plans, and other resources to aid in the development of applications. Information may include publicly available technical data, such as ground elevation information; property appraisal and land records; flood insurance studies; and hazard data. It may also include coordination with the program office to access protected data maintained by FEMA or another Federal Agency, such as disaster registration data. Standards may include identifying local or State adopted building codes relevant to the proposed mitigation measure. Plans can include identifying minimum design criteria and national consensus standards for the construction and/or performance of structures and facilities.
5. Assist with applying and adapting identified or acquired sources of data to existing FEMA tools such as the DTA Action Plan.
6. Gather, track and provide a summary of assistance delivered at each location which must include information such as, parties contacted, data obtained, standards and plans obtained, and assistance provided.
7. Assist with the development of schedules and resource plans.
8. Assist with developing or updating hazard risk assessments for mitigation projects.
9. Facilitate reviews of previous and existing efforts related to the project(s) to build a better understanding of potential projects.
10. Assist with the prioritization and conceptualization of potential projects. May involve feasibility exploration and identification of preliminary technical requirements but does not include engineering design.

11. Assist with the development of Building Resilient Infrastructure and Communities (BRIC) grant applications, including Benefit Cost Analysis support.
12. Provide guidance to communities on identifying possible relevant grant opportunities.

OBJECTIVE: 3 - Task Order Administration - Option 1:

This is a continuation of requirements listed in Objective 1. Base Period.

A meeting will be held to review base period actions and establish the workplan going forward.

OBJECTIVE: 4 - Provide technical support for Direct Technical Assistance (DTA) Communities - Option 1

This is a continuation of requirements listed in Objective 2. Base Period, with the following exceptions:

FEMA anticipates that approximately 34 additional communities and tribes will be targeted for service in Option Period 1.

GOVERNMENT PROVIDED DATA/RESOURCES

- Yes

If yes, indicate what data or resources will be provided to the contractor by the government.

- Government-Furnished Equipment (GFE)
- Direct Technical Assistance Action Plan per community
- Direct Technical Assistance Summary per community
- FEMA-approved state and local hazard mitigation plans
- Field assessment reports
- Direct Technical Assistance Program Support Material

- Technical Assistance Provider Webinar recording and PowerPoint slides

REQUIRED STANDARDS

- Yes

If yes, indicate the required standards for deliverables (i.e., compliance with statutes, regulations, FEMA guidance, etc.).

- All final documents should be 508 compliant.

CONSTRAINTS

- Yes

If yes, what does the contractor need to consider when developing an approach, such as: badging, schedule, access to project area as a result of damage, general logistics, systems compatibility, etc.?

- All staff who need access to a FEMA laptop or who will be interacting with community members whether by phone, virtual, email or in person will need to be badged.
- Confidentiality Agreement or Non-Disclosure Agreement for personnel.
- Contractor must coordinate site visits with the applicable FEMA Region prior to traveling.

ATTACHMENTS

- No

If yes, indicate the attachment title and provide a brief explanation of the contents of the attachment.

DELIVERABLES

List each deliverable type expected from this task order. Check all that apply.
Note: The Deliverables Clarification Form, Attachment A, must be completed to provide the required detail.

☐ Facilitation of services ☒ GIS product

☒ Reports & publications ☐ Technical drawings

☒ Guidance & presentations ☒ Excel spreadsheets Drawings

AUDIENCE

List the intended audience of the deliverable. Check all that apply.

☒ FEMA – Internal

☐ Technical audience

☒ General public

☒ Local communities

☒ Elected officials/policy makers

☒ Other: Consulting firms, tribal governments

☒ State government

COORDINATION

FEMA Project Monitor (Assigned by Division Director or Branch Chief)	Name	[redacted]
	FEMA Office	FEMA Headquarters - FIMA
	Mailing Address	400 C Street SW, Washington, DC 20472
	Phone	[redacted]
	Email	

Technical Monitor (Assigned by HMTAP Program Manager)	Name	[redacted]
	FEMA Office	FEMA Headquarters
	Mailing Address	400 C Street SW, Washington, DC 20472
	Phone	[redacted]
	Email	

Program Manager	Name	[redacted]
	FEMA Office	FEMA Headquarters
	Mailing Address	400 C Street SW, Washington, DC 20472
	Phone	[redacted]
	Email	

COR (Assigned by HMTAP Program Manager)	Name	[redacted]
	FEMA Office	FEMA/FIMA
	Mailing Address	400 C Street SW, Washington, DC 20472
	Phone	[redacted]
	Mailing Address	400 C. St. SW Washington, DC 20474

Administrative Requirements:

1. PRIVACY

To accomplish the tasks outlined in this contract, FEMA will share with the contractor the following PII data elements: first name, last name, email addresses, phone numbers, addresses and National Flood Insurance Program policy numbers of Hazard Mitigation Assistance Applicants/Sub applicants.

The information sharing outlined in this contract is authorized by the following PIA(s) DHS/FEMA/PIA-006 National Emergency

Management Information System Mitigation (MT) Electronic Grants (eGrants) System, DHS/FEMA/PIA-052 GMM SPARTA, DHS/FEMA/PIA-025 Hazard Mitigation Grant Program (HMGP) Routine Use F of SORN(s): DHS/FEMA-009 - Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs March 24, 2014 79 FR 16015, DHS/FEMA-004 Non-Disaster Grant Management Information Files, DHS/FEMA-009 Hazard Mitigation Disaster Public Assistance and Disaster Loan Programs, DHS/FEMA-008 Disaster Recovery Assistance Files

The contractors will have access to PII of first name, last name, email addresses, and work phone numbers of FEMA employees via Global Address List (GAL) by way of FEMA laptops use the information sharing is authorized by Routine Use F of DHS/ALL-014 Department of Homeland Security Personnel Contact Information" March 16, 2018, 83 FR 11780, PIA DHS/ALL-015 Web Portal, PIA DHS/ALL-059 Employee Collaboration Tool "

The contractor will limit access to the PII provided by FEMA under this contract only to the contractor's authorized personnel who need to know the information to accomplish the tasks outlined in this contract.

The contractor shall ensure no computer matching, as that term is defined in 5 U.S.C. § 552a (8), will occur for the purpose of establishing or verifying eligibility or compliance as it relates to cash or in-kind assistance or payments under federal benefit programs.

If at any time during the term of this contract any part of FEMA PII, in any form, that the contractor obtains from FEMA ceases to be required by the contractor for the performance of the contract, or upon termination of the contract, whichever occurs first, the contractor shall, within fourteen (14) days thereafter, promptly notify FEMA and securely return PII to FEMA, or, at FEMA's written request destroy, un-install and/or remove all copies of such PII in the contractor's possession or control, and certify in writing to FEMA that such tasks have been completed.

2. SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

1. *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.

2. *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);

   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).

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.

3. *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

(12) Safeguarding of Sensitive Information (MAR 2015)

(13) Information Technology Security and Privacy Training (MAR 2015)

(14) HSAR clause 3052.204-71 Contractor Employee Access

(15) 52.204-9 Personal Identity Verification Of Contractor Personnel (JAN 2011)

(16) 52.224-1 Privacy Act Notification (APR 1984)

(17) 52.224-2 Privacy Act (APR 1984)

4. *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.

5. *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.

    1. 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.

    2. 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. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

1. *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.

2. *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.

3. *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.

4. *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.

6. *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:

    1. Data Universal Numbering System (DUNS).
    2. Contract numbers affected unless all contracts by the company are affected.
    3. Facility CAGE code if the location of the event is different than the prime contractor location.
    4. Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
    5. Contracting Officer POC (address, telephone, email).
    6. Contract clearance level.
    7. Name of subcontractor and CAGE code if this was an incident on a subcontractor network.
    8. Government programs, platforms or systems involved.
    9. Location(s) of incident.
    10. Date and time the incident was discovered.
    11. Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level.
    12. Description of the Government PII and/or SPII contained within the system.
    13. Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system; and
    14. Any additional information relevant to the incident.

7. *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:

    1. Inspections,
    2. Investigations,
    3. Forensic reviews, and
    4. 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.

8. *Additional PII and/or SPII Notification Requirements.*

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

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

    1. A brief description of the incident.
    2. A description of the types of PII and SPII involved.

3. A statement as to whether the PII or SPII was encrypted or protected by other means.
4. Steps individuals may take to protect themselves.
5. 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
6. Information identifying who individuals may contact for additional information.

1. *Credit Monitoring Requirements*. If 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:

    1. Triple credit bureau monitoring.
    2. Daily customer service.
    3. Alerts provided to the individual for changes and fraud; and
    4. 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:

    1. A dedicated telephone number to contact customer service within a fixed period.
    2. Information necessary for registrants/enrollees to access credit reports and credit scores.
    3. 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.
    4. Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate.
    5. Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
    6. Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

2. *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*

3. 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 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.

Additional clauses for use in contracts

1) Safeguarding of Sensitive Information (MAR 2015)

2) Information Technology Security and Privacy Training (MAR 2015)

3) HSAR clause 3052.204-71 Contractor Employee Access

4) 52.204-9 Personal Identity Verification Of Contractor Personnel (JAN 2011)

5) 52.224-1 Privacy Act Notification (APR 1984)

6) 52.224-2 Privacy Act (APR 1984)

2. 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 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 while 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 SOW. 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 SOW. 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.

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.

3. 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.

4. 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.

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 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.

7. 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 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.

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 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 have 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 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.

8. 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 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.) always.

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.

The Contractor shall notify the FEMA COR of all terminations/resignations within five 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.

9. SECTION 508 REQUIREMENTS

Section 508 of the Rehabilitation Act (classified to 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.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

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, or any successor publication.

9.1 Section 508 Requirements for Technology Services

When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.

When modifying, installing, configuring or integrating commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.

When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at https://www.dhs.gov/compliance-test-processes.

Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

9.2 Section 508 Deliverables

Section 508 Test Plans: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.

Section 508 Test Results: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

Section 508 Accessibility Conformance Reports: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

Other Section 508 Documentation: The following documentation shall be provided upon request for ICT items offered through this contract:

- Documentation of features provided to help achieve accessibility and usability for people with disabilities.
- Documentation on how to configure and install the ICT Item to support accessibility.
- Documentation of core functions that cannot be accessed by persons with disabilities.
- Documentation of remediation plans to address non-conformance to the Section 508 standards.

1. Section 504 COMPLIANCE:

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.

[END OF SOO]