FEDERALLY FUNDED RESEARCH AND DEVELOPMENT (FFRDC) TECHNICAL EXECUTION PLAN (TEP)

U.S. Department of Homeland Security

Modernizing the Federal Emergency Management Agency (FEMA) Emergency Management Institute (EMI) Through the "EMI Anywhere" Initiative

Component/Office: Federal Emergency Management Agency (FEMA)
Directorate/Division: Emergency Management Institute (EMI)
FFRDC: Homeland Security Systems Engineering and Development Institute (HSSEDI)

Version: 1.2 – TEP43-23-0259 – Cost Proposal P23-743

Date: September 20, 2023, revised January 30, 2025

1. Challenge

Leadership for Federal Emergency Management Agency's (FEMA's) Emergency Management Institute (EMI) recognizes the need modernize the Institute's operations to better develop and support emergency managers anywhere they are, anytime in their careers. This initiative, referred to as "EMI Anywhere," requires robust tailored training and instruction for the emergency management community within federal, state, local, tribal, territorial, nonprofit, and private sector organizations. EMI Anywhere has the following six objectives:

- Expand virtual delivery by modernizing e-campus technologies and processes for online learning;
- Optimize the location of the main campus and expand into satellite campus partnerships with other federal organizations and universities;
- Revise and simplify the course catalog to be more relevant to the emergency management community and add certificate programs to address knowledge gaps in the profession;
- Develop and pilot an executive crisis leadership program that educates leaders on crisis leadership; roles, authorities, responsibilities, and capabilities of different levels of government and the private sector; and promotes networking;
- Facilitate and catalyze thought leadership for the emergency management profession among academics, researchers, practitioners, and policymakers to drive law, policy, strategy, doctrine, and education; and

- Transform EMI's current structure to replicate the organization and functions of modern educational institutions more closely by evolving towards a "war college" model.

2. Outcome(s)

EMI makes significant progress toward achieving the objectives of EMI Anywhere and FEMA achieves its strategic goal to "advance the emergency management profession by supporting curricula for federal comprehensive emergency management training, education, and professional development, accessible to whole community partners."[1]

3. Background

FEMA's mission is to help Americans before, during, and after disasters. As both the severity and frequency of disasters have increased, FEMA's role, operational tempo, and impact have also grown. This trend will likely continue as the nation faces the effects of climate change, pandemics, and other threats. One of FEMA's stated goals is to "promote and sustain a ready FEMA and prepared nation," including an objective to strengthen the emergency management workforce, led by FEMA's educational institutions.[2]

This is a new effort for HSSEDI. EMI is in the process of implementing EMI Anywhere, with varied progress across its six objectives to date.

4. Task Objective(s)

HSSEDI will directly support EMI's analysis, planning, and implementation of elements of three of the objectives of EMI Anywhere: expanding and modernizing delivery of virtual learning, determining the best possible locations for the main campus, and creating certificate programs and revising the course offerings and curricula (optional task) to address gaps.

4.1 Expand and Modernize EMI's Virtual Delivery (Base and Option Period)

HSSEDI will evaluate available virtual delivery platforms and provide support to EMI's selection and implementation of a system best suited for expansion of e-campus learning over short, medium, and longtime horizons. HSSEDI will also review EMI's existing processes for virtual learning and recommend improvements based on best practices and any specific needs of the emergency management community. Successful completion of this task will improve the accessibility, capability, and quality of the virtual learning experience.

---

[1] FEMA, *2022-2026 FEMA Strategic Plan: Building the FEMA our Nation Needs and Deserves.*

[2] Ibid.

4.2 Analyze Potential Future Locations for EMI's Main Campus (Base Period)

HSSEDI will provide analysis and recommendations to inform EMI's consideration of future locations for its main campus. Successful completion of this task will improve EMI's accessibility and grow its prominence in the emergency management community.

4.3 Create EMI Certificate Programs for Critical Topics (Base and Option Period)

HSSEDI will provide research, analysis, and development in support of creating new EMI certificate programs for identified critical topic areas. HSSEDI will assist in determining the certificates' course requirements and developing the curricula. Successful completion of this task will better align EMI's instruction with the priorities and needs of the emergency management community.

4.4 Additional research or studies as identified during the performance period that support implementing the NDEMU's Strategies and Plans (Optional Task)

5. Conduct ongoing research and analysis on emerging studies, policies, and data that align with and support the implementation of the President's agenda as applicable to NDEMU. Identify relevant findings throughout the performance period and integrate them into training materials, briefings, and strategic discussions to enhance policy execution and decision-making. Technical Approach / Analytic Methodology

To assist EMI with its objectives, HSSEDI will provide expertise in systems engineering, cloud and mobile computing, IT infrastructure and networking, decision analysis, program and risk management, acquisition, organizational change management, research in support of instructional development and design, and other disciplines as required. HSSEDI will also employ the services of outside experts in state-of-the-art approaches to delivering instruction and curriculum design for new and experienced emergency management professionals, if necessary.

5.1 Expand and Modernize EMI's Virtual Delivery (Base and Option Period)

In coordination with EMI stakeholders, HSSEDI will evaluate and recommend virtual learning platforms and operational best practices for virtual learning. HSSEDI will also support the procurement and rollout of the selected solution. Tasks will include:

- Collect current and project future demand for virtual learning at EMI. Solicit external subject-matter expertise on current best practices for virtual delivery and expectations of future technical and operational developments. Visit best-of-breed providers of education and instruction, such as the Army War College.

- Interview stakeholders to determine EMI's current and future user requirements for virtual learning, such as: accessibility; mobile and desktop user interface options; sharing of files and audio/video streams; compatibility with different lecture, lesson planning, and testing styles; and networking and collaboration features.
- Determine EMI's current and future technical requirements for virtual delivery, such as: infrastructure, system, subsystem, and interface requirements (e.g., with Learning Management Systems such as OPM USALearning and EMI's business systems); cloud architecture; cloud computing and storage deployment; synchronization with physical classroom learning; and cybersecurity.
- Assist EMI in drafting and posting a Request for Information (RFI) to gather data and clarification on vendor capabilities and future developments in the virtual learning market.
- Conduct an analysis of alternatives to assess a selection of a virtual delivery platform based on requirements, cost, security, and readiness for deployment. Test and evaluate potential solutions.
- Develop a procurement and implementation strategy, including timelines and cost estimates for acquiring the necessary services, hardware, software, networking, and storage solutions. Support the acquisition process.
- Review EMI's e-learning processes and establish metrics and responsibilities within the Institute that promote continuous operational improvement.
- Assist EMI to review and analyze DHS/FEMA enterprise systems/technology solutions. Provide feedback and recommendations.
- Facilitate meetings with EMI, FEMA Headquarters, FEMA Office of the Chief Information Officer (OCIO) to streamline the acquisition of the virtual delivery solution and development of artifacts.
- Assist EMI with the analysis of potential virtual delivery solutions and provide recommendations for continuing market research with the implementation of vendor technology demonstrations on the campus of the National Emergency Training Center (NETC), Emmitsburg, Maryland, in Building K Room 302.

5.2 Analyze Potential Future Locations for EMI's Main Campus (Base Period)

In coordination with EMI leadership, HSSEDI will perform an analysis of alternatives to assist EMI in considering future locations for its main campus. Tasks will include:

- Determine campus requirements, such as: proximity to students and agency/university partners, access to talent, capacity (e.g., classrooms, housing), bandwidth availability, readiness for instruction to begin.
- Visit candidate locations to gather additional information and engage with area leadership

and potential partners.

- Conduct a business case for each potential campus location based on requirements, costs, economic benefits, and timeliness. Recommend a course of action for EMI.

5.3 Create EMI Certificate Programs for Critical Topics (Base and Option Period)

HSSEDI will conduct a stakeholder analysis and environmental scan to inform EMI's addition of certificate programs to address knowledge gaps in the profession, with an emphasis on disaster logistics and supply chain management. Tasks will include:

- Interview experts from EMI, FEMA, and other relevant organizations to solicit input on certificate construction and curricula requirements.
- Research and interview other domestic and international institutions (including FEMA) providing emergency management instruction to gain insight on the certificates they offer and to avoid creating unnecessary redundancies.
- Recommend which EMI courses be added, removed, or modified to meet certificate program requirements.
- Engage with internal and external experts to help identify existing or develop new, relevant subject matter that will be used by EMI instructional design staff to develop curricula supporting future certificate programs.
- Recommend identified critical topic areas of disaster logistics and supply chain management for an independent study (IS) course.
- Analyze and identify existing courses to comprise the foundational and elective stages of the disaster logistics and supply chain management certificate program.
- Recommend an outline and design for the disaster logistics and supply chain management certificate program capstone informed by the proposed IS topics and foundational, and elective courses.
- As time permits under the current PoP, analyze and identify instructor competencies for the disaster logistics and supply chain management certificate program capstone.

5.4 Additional research or studies as identified during the performance period that support implementing the NDEMU's Strategies and Plans (Optional Task)

HSSEDI will analyze EMI's current curricula and conduct an environmental scan to inform the revision and modernization of EMI's course catalog to address knowledge gaps in existing instruction. Tasks will include:

- Review existing EMI instruction and programs.
- Interview experts from EMI, FEMA, and other educational organizations to identify gaps, redundancies, and other issues with the current EMI course catalog.

- Interview other domestic and international institutions (including FEMA) providing emergency management instruction to gain insight on their related courses, programs, and curricula.
- Recommend which EMI courses be added, removed, or modified to address gaps.
- Engage with internal and external experts to help identify existing relevant subject matter that will be used by EMI instructional design staff to develop curricula supporting future certificate programs.

6. Key Words

Type of Work

Technology modernization, decision analysis, education, acquisition, business case analysis, capability standup, partnerships, digital transformation.

Benefit of Work

Enhances EMI's ability to advance the emergency management profession by supporting curricula for federal comprehensive emergency management training, education, and professional development, accessible to whole community partners.

Subject of Interest

Training and education of the emergency management workforce.

7. Focus Area and Mission Alignment

Table 1 below aligns the percent of the total projected staff years of technical effort (STE) allocations to the IDIQ focus areas and DHS Quadrennial Homeland Security Review (QHSR) missions.

HSSEDI proposed total STE: 3.92 Base and optional work (18 month POP)

DHS Management Directive 143-04, "Establishing or Contracting with FFRDCs and National Laboratories" defines a STE as 1,810 hours of paid effort for technical services.

Table 1: Focus Areas to the QHSR Mission Areas Relationship Matrix

	QHSR Missions					
HSSEDI Focus Areas	Mission 1: Prevent Terrorism and Enhance Security	Mission 2: Secure and Manage Our Borders	Mission 3: Enforce and Administer Our Immigration Laws	Mission 4: Safeguard and Secure Cyberspace	Mission 5: Strengthen National Preparedness and Resilience	Mission 6: Maturing and Strengthening Homeland Security
1. Acquisition Planning and Development	0%	0%	0%	0%	0%	0%
2. Emerging Threats, Concept Exploration, Experimentation and Evaluation	0%	0%	0%	0%	0%	0%
3. Information Technology and Communications	0%	0%	0%	0%	45%	0%
4. Cyber Solutions / Operations	0%	0%	0%	0%	0%	0%
5. Systems Engineering, System Architecture and Integration	0%	0%	0%	0%	45%	0%
6. Technical Quality and Performance	0%	0%	0%	0%	0%	0%
7. Independent Test and Evaluation	0%	0%	0%	0%	10%	0%

HSSEDI shall provide the following deliverables (predicated in calendar days) according to Table below, and the most current Project Management Plan (PMP), as approved by the Project Manager and FEMA Contracting Officer or COR.

Table 2: Deliverables

Scope Ref.	Deliverable Name	Delivery Date
5.0.1	Project Management Plan (PMP) (Draft)	15 days after award
5.0.2	Project Management Plan (PMP) (Final)	30 days after award

5.0.3	Task Order Project Kickoff Briefing	Within 30 days of award date
5.1	Final Report Assessing and Recommending Virtual Learning Platforms	Within 12 months of award date
5.2	Final Report Assessing and Recommending Campus Locations	Within 9 months of award date
5.3	Final Report Recommending Certificate Program Courses and Curricula	Within 12 months of award date
5.1, 5.3, 5.4	Project Close Out Report Summation of Work Tasks 1, 3, & 4 from Oct 2024 – Mar 2025	Within 18 months of award date

HSSEDI shall provide all deliverables under this task order directly to the S&T FFRDC PMO ([redacted], the Task Order PM, TPOC, and Task Order COR. An unclassified abstract, 100 to 200 words in length, and at least five keywords, or a completed Standard Form 298, "Report Documentation Page," shall accompany each deliverable as indicated in Table 2. deliverable. Note that the Report Documentation Page will identify the approved release distribution level (e.g., distribution is unlimited; distribution authorized to US Government agencies only; etc.).

HSSEDI shall deliver a monthly status report by the 23rd of the following month containing metrics pertaining to financial, schedule, technical progress, deliverable status, and risk information related to the task. The HSSEDI task lead and the task order COR as needed will discuss relevant issues in evaluating the task priorities for the next period; and update the program plan as necessary.

9. Assumptions

- Deliverables will be primarily electronic unless otherwise directed by the task sponsor.
- The current estimate is based on information to date. HSSEDI will work collaboratively with the government to clarify and adjust if needed, focus and/or resource needs associated with the specific tasks, subtasks, and formal deliverables, informed by budget and schedule constraints, while remaining within overall project scope.
- The government will be responsible for managing any necessary formal government review and concurrence process that may derive from deliverables associated with these tasks.
- FAR section 4.7 Contractor Records Retention requires contractors to maintain records for 3 years following the final payment on a task order. Along with this and other audit

obligations, MITRE must maintain a record of all unclassified deliverables, formal and informal. To meet these requirements, HSSEDI intends to use its archive site (known as DOV) located in the HSSEDI Enclave to collect and store all unclassified deliverables, regardless of where the deliverables are developed.

- FEMA and EMI will provide HSSEDI access to relevant data sets, subject matter experts and supporting integration partners and contractors.
- FEMA suitability approval may take 60 business days from date of contract award (the paperwork submission will start within 5 business days of award).
- FEMA and EMI will provide government furnished equipment to the HSSEDI team members to facilitate task execution from HSSEDI facilities.
- HSSEDI SMEs (FEMA cleared) supporting this task (outside of DC Metro area) with specialized skillsets will provide subject matter expertise, and technical outreach to commercial, academic, and other government components for the analysis work through MITRE-issued laptops.

10. Travel

Travel may be necessary to meet and coordinate interagency exchanges of information and to collect data for this task. HSSEDI shall provide trip reports, if requested, to the task order COR for all non-local travel within 30 days of completion of travel.

Long Distance Travel base and option

From	To	No. of Trips	No. of Days per Trip
MITRE McLean	Emmitsburg, MD (EMI HQ)	5	2
MITRE McLean	Summit Point, WV. - Candidate Locations for EMI's Main Campus	1	3
MITRE McLean	Seattle, WA. - Candidate Locations for EMI's Main Campus	1	3
MITRE McLean	Huntsville, Al. - Candidate Locations for EMI's Main Campus	1	3
MITRE McLean	Charleston, SC. - Candidate Locations for EMI's Main Campus	1	3
MITRE McLean	Dallas, TX. - Candidate Locations for EMI's Main Campus	1	3

MITRE McLean	Newport, RI. - Other Best-of-Breed Institutions Providing Instruction on Emergency Management	1	3
MITRE McLean	USAF Academy, CO. - Other Best-of-Breed Institutions Providing Instruction on Emergency Management	1	3
MITRE McLean	Fort Leavenworth, KS. - Other Best-of-Breed Institutions Providing Instruction on Emergency Management	1	3
MITRE McLean	College Station, TX. - Other Best-of-Breed Institutions Providing Instruction on Emergency Management	1	3
MITRE McLean	Monterey, CA. - Other Best-of-Breed Institutions Providing Instruction on Emergency Management	1	3

- Total Number of Trips (All Travelers): 15
- Total Number of Travel Days (All Travelers): 40

The task order COR must approve all foreign travel. Foreign travel must be approved at least 30 days (for unclassified visits) or 45 days (for classified visits) in advance of the planned travel event.

Travel, including local non-commuting travel, shall be reimbursed in accordance with the Federal Travel Regulation. Daily commuting costs shall not be reimbursed. Long-distance travel not specified in this Task Order must be pre-approved by the Task Order CO or COR.

11. Period of Performance

The period of performance (POP) is 18 months from date of task order award with optional tasking starting minimally within six months before POP end.

12. Security Requirements.

This Task Order will require access to the following information:

X 1. Unclassified, no markings
X 2. Sensitive but Unclassified (SBU), For Official Use Only (FOUO)
X 4. Personally Identifiable Information (PII)

12.1 Security requirement #2 (SBU, FOUO) – All unclassified "For Official Use Only" (FOUO) work is expected to occur at the "medium" level per the National Institute of Standards and Technology (NIST) 800-60 (Federal Information Processing Standard (FIPS) Security Categorization) and the Federal Information Security Management Act (FISMA). Any work at the "high" FOUO level per the FISMA, or any work at the classified level, shall be performed on a stand-alone computer system accredited in accordance with the FISMA and applicable DHS policies.

12.2 Security requirement # 2 (SBU, FOUO) – The FFRDC shall adhere to all applicable government laws, regulations, orders, guides, and directives pertaining to classified, Sensitive But Unclassified (SBU), FOUO, or personally identifiable information. The contractor shall safeguard SBU, FOUO information specifically in accordance with DHS Management Directive 11042.1 and in compliance with HSAR Class Deviation 15-01 Safeguarding of Sensitive Information.

12.3 Security Requirement #4 (PII) – To accomplish the tasks outlined in this TEP, FEMA will share with the FFRDC the following PII data elements: name, work email address, and work phone number for FEMA employees, FEMA contractors, and external stakeholders in the State, Local, Tribal, and Territorial (SLTT) community. The information sharing outlined in this TEP is authorized by the following System of Records Notice(s) and Routine Use(s): <TBD pending PTA adjudication>. The information sharing outlined in this TEP is covered in the following Privacy Impact Assessment(s): <TBD pending PTA adjudication>. The FFRDC will limit access to the PII provided by FEMA under this TEP only to the FFRDC's authorized personnel who need to know the information to accomplish the tasks outlined in this TEP. The FFRDC shall ensure no computer matching, as that term is defined in 5 U.S.C. § 552a(o), 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 FFRDC obtains from FEMA ceases to be required by the FFRDC for the performance of the contract, or upon termination of the contract, whichever occurs first, the FFRDC 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.

12.4 Authorized IT Environments

The HSSEDI team will use their MITRE corporate IT environment for HSSEDI contracts management and administrative support for activities including:

- Time reporting
- Financial management
- Contract management
- Monthly status reports
- Non-DHS Sensitive project work

Sensitive HSSEDI work described in the TEP will be performed in IT environment(s) authorized by DHS. These may include, a) HSSEDI IT Enclave, b) DHS infrastructure (e.g., LAN-A), and/or c) other authorized environment(s)(e.g., classified networks).

12.5 DHS Furnished Information

a) DHS/FEMA will provide unique information, materials, and forms to the Contractor as specified under this task order. Such DHS/FEMA provided information, materials, and forms shall remain the property of DHS/FEMA, unless otherwise indicated in writing by DHS, and may not be distributed beyond the FFRDC's project performers without DHS's prior written permission.

b) The DHS/FEMA COR identified in this task order will be the point of contact (POC) for identifying required information to be supplied by DHS/FEMA.

12.6 Privacy Compliance Requirements

The Government Program Manager will coordinate with the appropriate DHS component's Privacy Office (i.e., CBP, USCIS, S&T, etc.) to determine if a Privacy Threshold Analysis (PTA) is required prior to the start of performance. In those instances, the performer shall support the development of compliance related documentation and meet privacy requirements. Please have your privacy office reach out to S&T Privacy to see what documentation is available.

12.7 Personnel Security Requirements

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

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

Disclosure of Classified or Unclassified Information training.

Access to the training can be obtained at: Unauthorized Disclosure of Classified Information and Controlled Unclassified Information (usalearning.gov)
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 OPSEC Awareness for Military Members, DOD Employees and Contractors (usalearning.gov)

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: Insider Threat Awareness (usalearning.gov)

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

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

1. Be aware of and comply with the safeguarding requirements for "For Official Use Only" (FOUO) information as outlined in this directive.
2. Participate in formal classroom or computer-based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.

3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

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

Foreign Travel and Government-Issued Equipment

Per DHS and FEMA IT policy, FEMA employees and contractors are not authorized to take government-issued equipment, including cell phones, computers, or tablets such as iPads, outside of the United States regardless of the reason for travel. If government-issued equipment is required for official foreign travel, FEMA government employees may request a temporary loaner device through the Mobility Service Center, Office of the Chief Information Officer, Service Center for the duration of their trip. FEMA contractors must contact their contracting officer's representative (COR) for further guidance.

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

Background Investigations

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

Low Risk without Information System Access

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

Low Risk with Information System Access

Contractor personnel occupying positions or performing functions with a Low Risk

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

Moderate Risk

Contractor personnel occupying positions or performing functions with a Moderate Risk designation shall undergo a Tier 2 Suitability Background Investigation (T2) and must 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 121-3-16, "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 of the above document and Standard Form 85P, which must be completed electronically through the Office of Personnel Management's e-QIP system. The Contractor is responsible for ensuring that all contractor personnel timely and properly submit all required background information. Once contractor personnel have properly submitted the complete package of all required background information, FEMA's Personnel Security Division, at its sole discretion, may grant contractor personnel temporary eligibility to perform work under this contract prior to completion of the full background investigation if the Personnel Security Division's initial review of the contractor personnel's background information reveals no issues of concern. In such cases, FEMA's Personnel Security Division will provide notice of such temporary eligibility to the COR who will then notify the Prime Contractor, at which time the identified contractor personnel will be temporarily eligible to begin work under this contract. Neither the Prime Contractor nor the contractor personnel has any right to such a grant of temporary eligibility. The grant of such temporary eligibility shall not be considered as assurance that the contactor personnel will remain eligible to perform work under this contract upon completion of and final adjudication of the full background investigation.

Upon favorable adjudication of the full background investigation, FEMA's Personnel Security Division will update the contractor personnel's security file and take no further action. In any instance where the final adjudication results in an unfavorable determination FEMA's Personnel Security Division will notify the contractor personnel directly, in writing, of the decision and will provide the COR with the name(s) of the

contractor personnel whose adjudication was unfavorable. The COR will then forward that information to the Contractor. Contractor personnel who receive an unfavorable adjudication shall be ineligible to perform work under this contract. Unfavorable adjudications are final and not subject to review or appeal.

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

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

FACILITY ACCESS

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

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

Contractor personnel shall not receive a FAC until they have submitted a SF 87, "Fingerprint Card," and an OF306, Declaration for Federal Employment, and receive approval from FEMA PSD. Contractor personnel using a FAC for access to FEMA

facilities must be escorted in Critical Infrastructure areas (i.e., server rooms, weapons rooms, mechanical rooms, etc.) at all times.

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

SEPARATION FROM CONTRACT

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

13. Safeguarding/Storage:

a. No safeguarding/storage needed at the FFRDC.

14. Other Contract Details

In accordance with the language in the HSSEDI contract, the following sections are repeated here for awareness and should not be changed. If they are changed, the language in the IDIQ takes precedence.

14.1 FFRDC Personnel

Personnel provided by HSSEDI will have the skills and technical background necessary to successfully complete the tasks described in this plan. HSSEDI shall implement and

manage the technical approach, organizational resources, management, and quality controls to be employed to meet the cost, performance and schedule requirements throughout task order execution.

14.2 Food and Drink.

HSSEDI shall not charge any expense for food, snacks, or drink as part of holding task related meetings, conferences, or gatherings; however, this prohibition does not prevent the contractor from charging meals and incidental expenses as part of authorized travel expenses.

14.3 Meetings and Workshops

All necessary conference approvals should take place prior to HSSEDI's attendance at any conference in support of the sponsoring component. The component user should follow the conference approval process per the guidance set-forth under DHS Financial Management Policy Manual (FMPM Section 7.10) and any component-specific policies and procedures and provide a copy approval(s) to the FFRDC.

HSSEDI may interview and conduct workshops of recognized subject-matter experts, including non-federal experts, to gather the expert's individual knowledge and experience regarding the current state of the art of the technical issues relating to this task, and to foster the building of a long-term collaboration between the individual subject matter experts and HSSEDI on the issues relating to the experts' areas of expertise. The workshops or other interaction with non-Federal experts will be for the purpose of collecting the views of the individual experts, not to result in a consensus of those experts. HSSEDI shall produce an objective assessment on the technical merits of the data and/or experts' views espoused in these meetings; and include an evaluation of the strengths and weaknesses of the various discussion points provided by individuals.

HSSEDI may organize meetings/workshops related to the task with federal officials on behalf of the user; however, federal government personnel will approve the agenda and will chair any federal intra-agency/inter-agency meetings. HSSEDI shall produce an objective assessment on the technical merits of individual and any consensus findings and recommendations discussed in these meetings; and include an evaluation of their strengths and weaknesses of the various discussion points.

14.4 Inherently Governmental Functions

As defined under FAR subpart 7.503 (d) and additionally as described in the Office of Federal Procurement Policy (OFPP) Letter 11- 0 I, Performance of Inherently Governmental and Critical Functions (76 Fed Reg 56227), the FFRDC may perform certain closely associated with inherently Governmental functions. However, in accordance with Federal Acquisition Regulation (FAR) 7.503(c)(20) and Homeland Security Acquisition
Manual 3037.103(e), the FFRDC shall not draft Congressional testimony, responses to Congressional correspondence, or agency responses to audit reports from the Inspector General, the Government Accountability Office, or other Federal audit entity. Furthermore, in accordance with FAR 7.503(c)(12)(ii), FFRDC employees, subcontractors, and/or consultants will not be voting members on any DHS source selections. When applicable, FAR clause 52.203-16, "Preventing Personal Conflicts of Interest," as included in the IDIQ contract, will apply to this Task Order.

14.5 Out of Scope Work

The following types of work are out of scope for the FFRDC to perform. More specific types of work that are out of scope are found in the relevant IDIQ contract:

- Performance of any services and functions as defined under FAR Subpart 7.5 "Inherently Governmental Functions," specifically subparts 7.503 (a), (b) and (c).
- Performance of any Systems Engineering and Technical Assistance (SETA) type work, particularly where such work is directly for staff augmentation and of a general support nature where the specific type and quantity of deliverables are undefined.
- Preparation of any Independent Government Cost Estimates (IGCEs).
- Participation in any Source Selection Evaluation or any other membership body where voting and/or ranking of proposals will lead to a subsequent monetary or contract award. The FFRDC may provide independent technical evaluation of proposals in support to a Source Selection Evaluation body but may not provide any ranking, voting or other assigned ordering or selection criteria other than commenting on the technical merit of a particular proposal or proposal section(s). Use of the FFRDC in evaluating an offeror's proposal MUST BE DISCLOSED IN THE SOLICITATION OF PROPOSALS and the offeror(s) given the opportunity to affect non-disclosure agreements and/or withdraw their offer(s), otherwise the FFRDC may not participate.
- Delivering recurring compliance training to DHS employees, particularly that which could reasonably be considered staff augmentation services, is not allowed. Training

associated with the transfer of skills from the FFRDC to DHS is acceptable, as long as such training is non-recurring (i.e. train the trainer) and is not intended to be part of a formal established training program. Waivers to this may be requested from the FFRDC COR. Seminars, workshops, and short-courses intended to extend the access and awareness of FFRDC research, research methods, and data sets to practitioners across the Homeland Security Enterprise to assist them in improving mission effectiveness and efficiency is permissible.

- Software and/or hardware development or other manufacturing unless such development is associated with a prototype demonstration or other proof of concept system and not intended to be a permanent solution or in response to formal requirements.

15. Publications and Communications Concerning Work Performed

In accordance with the language in the HSSEDI FFRDC contract, the following statement is repeated here for awareness and should not be changed. If it is changed, the language in the IDIQ takes precedence.

The FFRDC shall mark all technical data or computer software pursuant to the terms of the IDIQ Contract. This will include, for copyrighted works, an appropriate notice acknowledging DHS's sponsorship of the work, license rights, and the appropriate copyright notice as detailed in the IDIQ Contract.
The DHS desires widespread dissemination of the results of funded non-sensitive research and does not seek to undermine the independence or objectivity of the FFRDC or FFRDC operator in anyway. The FFRDC therefore will generally seek public release approval for the results of nonsensitive research. Thirty (30) days prior to release, the FFRDC will first ask for the task order COR's and CO's agreement that the research product is suitable for release. The FFRDC contract governs the scope of the review. Specifically, this review is strictly a mechanism by which the
Department identifies the inclusion of Sensitive Information, as defined in the IDIQ contract, Section I.13(a). The review does not include a determination of the FFRDC's analytical conclusions, final findings, or analytical outcomes.

- Are you interested in releasing information publicly from this research?
  No, at the time of award no research is intended to be released. If this changes during the conduct of this research effort, HSSEDI will use the appropriate Public Release Process to gain concurrence.
- If you don't want to release the results, is HSSEDI able to release info about the methodology to the other components or the public? *N/A*

- What is the desired audience for the release of info? Component only/all of DHS/public release? *N/A*
- Do you want an outreach event as part of the release? *N/A*
- Would you be interested in having the S&T FFRDC PMO assist with the release of favorable results? *N/A*

16. DHS Furnished Facilities, Supplies and Services (<<Completed by User>>)

If work at FEMA (FEMA) is necessary for the services being performed under this Task Order, such facilities will be provided at offices at the appropriate location. Parking facilities are not provided. Basic facilities such as workspace and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable and general purpose office supplies) will be provided to HSSEDI personnel.
DHS Furnished Property – a quarterly report of all S&T property should be submitted to the COR |FFRDC of all of the equipment purchased on behalf of the Government, and Government Furnished equipment being utilized by HSSEDI.

Subsequently a yearly report of all Government Furnished Equipment shall be provided to the COR | FFRDC. The COR | FFRDC will need a property form filled out for all S&T Contractor Acquired Equipment /Property or purchases on behalf of the Government for insertion into the S&T property management system (SAMS). This insertion will need to include the property form filled out in its entirety, paid invoice(s) showing the property purchase and a picture of the current state of that property.

a) Additional DHS property will not be provided to the FFRDC unless otherwise agreed. If DHS property is provided to the FFRDC for task performance, the FFRDC shall maintain property records, sending a yearly report of all items currently attached to the task order to the COR|FFRDC and the Program Manager and a disposition of the property must be completed at the end of the period of performance.
b) Before purchasing any individual item equal to or exceeding $5,000 that is required to support technical tasks performed pursuant to this Task Order, that has not already been accepted by the Government with the issuance of the Task Order, HSSEDI shall obtain prior written consent from the Program Manager, task order Contracting Officer, and task order COR. HSSEDI shall maintain any such items according to the IDIQ Contract's property accountability procedures, and FAR Part 45.
c) All DHS/GFP/GFE (IT equipment, building passes etc.) must be returned at the conclusion of the task order in accordance with component's procedures.

d) If any GFP/GFE is not returned, a report of survey must be submitted to the COR and Project Manager, referencing the DHS equipment number, pass or card number, name of individual to whom equipment was issued, and the last known location of property. Contractors who lose a badge will be required to fill out an additional lost badge form.

17. Invoices

Contractors will use Standard Form 1034 (Public Voucher for Purchases and Services Other Than Personal) located at http://www.gsa.gov/portal/forms/type/SF when submitting a payment request. A payment request means any invoice or request for contract financing payment requesting reimbursement for supplies or services rendered. The Contractor shall not be paid more frequently than on a monthly basis.

Contractors must submit vouchers electronically in pdf format to the FEMA Finance Center at [redacted]. A copy of the voucher must be submitted electronically to the contracting officer identified within this contract. The submission of vouchers electronically will reduce correspondence and other causes for delay to a minimum and will facilitate prompt payment to the Contractor.

18. Points of Contact

Government POCs	Corresponding HSSEDI POCs
Program Manager [redacted]	**HSSEDI Task Lead** [redacted]
Contracting Officer's Representative [redacted]	**HSSEDI Department Manager** [redacted]
Alternate COR [redacted]	

[redacted]

Contract Officer

TBD

HSSEDI Contracts Lead/Manager

[redacted]

Suitability/Fitness Point of Contact

[redacted]

HSSEDI Security Staff

[redacted]

19. 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);

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.

(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 4300A Policy Directive (Version 13.3, February 13, 2023)

(3) DHS Policy Directive for Safeguarding Sensitive Personally Identifiable Information

(4) DHS Instruction Policy Directive 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(5) DHS Information Security Performance Plan (current fiscal year)

(6) DHS Privacy Incident Handling Guidance

(7) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(8) 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

(9) 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 Policy Directive (Version 13.3, February 13, 2023) provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Policy Directive for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Policy Directive 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 110006, 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 4300A Policy Directive (Version 13.3, February 13, 2023), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate

Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

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

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

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

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

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

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

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

Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

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

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Policy Directive 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 USCERT 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 Policy Directive Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);

(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the Government PII and/or SPII contained within the system;

(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

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

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

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

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews, and

(iv) Data analyses and processing.

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

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

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

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

(i) A brief description of the incident;

(ii) A description of the types of PII and SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

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

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

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a

company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

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

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

(k) "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.

20. 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 email 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/dhssecurity-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.

21. 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:

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

C. Requirements
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.

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.

In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

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.

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).

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.

The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with FEMA policy.

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.

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.

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.

22. Information Sharing

To accomplish the tasks outlined in this contract, FEMA will provide the contractor access to the Modernizing the FEMA EMI Through the "EMI Anywhere" Initiative and the following PII data elements (name, work email address and work phone numbers).

The information sharing outlined in this contract is authorized by the following System of Records Notice(s) and Routine Use(s):

DHS/ALL 016 Correspondence Records September 26, 2018 83 FR 48645; Routine Use G.
DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792; Routine Use F.

The information sharing outlined in this contract is authorized by the following Privacy Impact Assessments:

DHS/ALL-015 Web Portal
DHS/ALL-059 Employee Collaboration Tool
DHS/ALL-012b Email Secure Gateway
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(o), 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.

23. DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

(a) All developed solutions and requirements shall be compliant with the HLS/FEMA EA.

(b) All IT hardware and/or software shall be compliant with the HLS/FEMA EA Technical Reference Model (TRM) Standards and Products Profile.

(c) Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

(d) Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01[1] and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

(e) Applicability of IPv6 to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

24. Section 508 Compliance

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.

Section 508 Requirements for Technology Services

1. When providing installation, configuration or integration services for ICT, the Contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

2. 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.

3. 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.

4. 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.

5. When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under

"Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester

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

Section 508 Deliverables

1. **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.

2. **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.

3. **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 of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

4. **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

26. OCIO CISO Cyber-Supply Chain Risk Management (C-SCRM) Requirements

a. Definitions

i. Component: a unit defined by the supplier that connects to and functions as part of the product. For software products, a component is a unit of software defined by a supplier at the time the component is built, packaged, or delivered. For hardware, a component is one hardware unit designed to connect to and function as part of a larger product.

ii. End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

iii. End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

iv. Information and Communications Technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

v. Product: part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.

b. Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product

i. The contractor shall provide new equipment unless otherwise formally approved by the Government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the Government. In the event that a shipped OEM product, or part or component of that product, fails, all replacements must be new (i.e., non-refurbished, not previously used) OEM.

ii. The contractor may provide previously-used OEM products only with written Government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

c. Accounting of Components in ICT Products

i. The contractor shall provide and maintain a list of components for each product used in performance of the contract, including through subcontracts or other arrangements. This list for each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.

ii. The contractor shall notify the Government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to reflect the new version of the software. This includes software builds to integrate an updated component or dependency.

iii. For software products, the contractor shall provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract, and replaced when End of Support (EoS) is reached.

iv. A contractor using team members in performance of the contract (e.g., subcontractors or other service providers) shall ensure that the standards for the accounting of components in this subsection are met by team members.

d. Supply-Chain Transport

i. The contractor shall use formal, documented and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.

ii. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance, and make available for inspection upon request of the Government.

iii. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.

iv. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

v. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Changes to Ownership and Control

The Contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any significant changes to corporate ownership or control from contract award through final delivery or the end of the period of performance. A significant change would be one in which a change occurs in the individuals or entities who, directly or indirectly, either (1) exercises substantial control over an entity, or (2) owns or controls at least 25 percent of the ownership interests of an entity.

27. FedRAMP Certified Requirements

- **The proposed cloud solution must be FedRAMP certified. Reference:** Federal Risk and Authorization Management Program (FedRAMP), http://www.fedramp.gov:
- National Institute of Standards and Technology (NIST), U.S. Department of Commerce (DOC), Special Publication (SP) 500-292, *NIST Cloud Computing Reference Architecture*, September 2011.
- NIST, U.S. DOC, SP 800-145, *NIST Definition of Cloud Computing*, September 2011.
  (a) Cloud computing. All use of cloud computing products or services that process unclassified information must comply with the FedRAMP Authorization Act, 44 U.S.C. Section 3607 et. seq. The following requirements apply when using cloud computing to provide information systems or services in the performance of the contract.
  i. Cloud computing security requirements. The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with FedRAMP Security Authorization Requirements unless notified by the Contracting Officer that this requirement has been waived by the Agency Chief Information Officer.
  ii. Cloud computing continuous monitoring. The Contractor shall maintain an adequate continuous monitoring capability based on the FedRAMP Security Authorization Requirements including processes described in the NIST Special Publication (SP) 800-137, Information

Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations and governed by the FedRAMP Continuous Monitoring Strategy Guide.

iii. Cloud computing services cyber incident reporting. The Contractor shall report all cybersecurity incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted according to FedRAMP Security Authorization Requirements, published FedRAMP Incident Communications Procedures, and Federal Incident Notification Guidelines for submitting incident notifications to CISA using the CISA incident reporting form (https://us-cert.cisa.gov/report).