Performance Work Statement (PWS)
National Preparedness and Assessment Division (NPAD)
Program Support Services
Revision Date: 05/15/2025

1.0 Background

FEMA's National Preparedness Directorate (NPD) provides the doctrine, programs, and resources necessary to prepare the Nation to prevent, protect, mitigate, respond to, and recover from disasters; while minimizing the loss of lives, infrastructure, and property.

As a division within NPD, the National Preparedness Assessment Division (NPAD) provides the analyses and assessments necessary to measure and communicate the effectiveness of preparedness investments, activities, and accomplishments and to drive continuous improvement. NPAD has three branches that carry out its work: Assessments and Analytics, Continuous Improvement Integration, and Measures and Standards. Each has a specific role that supports Whole Community preparedness by leading analyses and assessments that shape strategic investments, activities, and decisions; measuring grant effectiveness; driving national preparedness priorities; and communicating progress toward becoming a more secure and resilient Nation. NPAD's mission contributes to the missions of NPD, FEMA, and DHS by conducting analysis and communicating the results that lead to strategic, policy, operational, and financial decisions about preparedness. These decisions inform how FEMA and its stakeholders build, sustain, and deliver the capabilities needed to be a secure and resilient Nation. The purpose of this task order is to provide the support necessary to assist NPAD in assessing national preparedness.

The Post-Katrina Emergency Management Reform Act of 2006 (PKEMRA) requires that "states receiving Federal preparedness assistance administered by the Department shall report on their levels of preparedness" and that FEMA identify, generate, and disseminate lessons learned, best practices, and after-action reports (AARs) from real world incidents and emergency management exercises at all levels of government. In addition, the Disaster Recovery Reform Act of 2018 (DRRA) requires FEMA to "complete a national preparedness assessment of capability gaps at all levels based on tiered, capability-specific performance objectives to enable prioritization of grant funding" and "identify the potential costs for establishing and maintaining those capabilities at each level and determine what capabilities Federal agencies should provide."

Based on these authorities, NPAD is responsible for annually producing the National Preparedness Report, assessing State compliance with the National Preparedness System, National Incident Management System, the National Response Framework (NRF), and other related plans and strategies; managing and implementing the Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR), which provides an assessment of current capability levels against defined targets at both the community and national levels; and supporting the assessment of resource needs to meet preparedness priorities. NPAD also manages the Continuous Improvement Program (CIP), an essential component of FEMA's assessment and improvement activities. Within this program, NPAD tracks corrective

actions stemming from disasters and analyzes trends to facilitate remedies to recurring issues that challenge FEMA's ability to respond to and recover from future incidents. The Measures and Standards Branch (MSB) leads Monitoring, Evaluation, and Learning (MEL) activities and conducts performance monitoring, case studies, qualitative and quantitative analyses, program evaluations and other evaluative studies, of all Resilience programs including for FEMA's preparedness grant programs. MSB is also responsible for contributions to the DHS learning agenda and meeting the standards of the Evidence Act.

1.1 Scope

The scope of this Performance Work Statement (PWS) is to support NPAD in ompleting the following known products and services that align to the mission objectives listed above. Those known deliverables are listed in Section 2.8. The contractor will also support any products or deliverables identified during the period of performance that align to the mission objectives and can be completed consistent with the tasks outlined in Section 2.0 Specific Responsibilities/Tasks. Supports the division in achieving the above development of the following deliverables and other assigned by the COR.

NPAD consists of 3 branches Continuous Improvement Integration Branch, Measures and Standards Branch, and Assessments and Analytics Branch.

Assessments and Analytics Branch

The Assessments and Analytics Branch (AAB) is responsible for collecting, analyzing, and conducting preparedness and risk assessments across National, State, Territorial, Tribal, and local levels, which provide a foundation for the National Preparedness System. AAB leads the development, annually, of the National Preparedness Report, which summarizes and communicates the preparedness capabilities of Federal, State, and local actors and seeks to answer the question of "how prepared are we, as a nation?"; implements and analyzes the results of the Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Revie (SPR), which supports jurisdictions in assessing their current capabilities and prioritizing their strategic preparedness needs; and leads the development of the National THIRA and SPR, to inform decisions concerning the capabilities the Nation must build and sustain to prepare for catastrophic incidents.

Continuous Improvement Integration Branch

Continuous Improvement Program (CIP) within the Continuous Improvement Integration Branch enhances the Agency's culture of continuous improvement of service delivery to survivors and stabilization of critical lifelines throughout the disaster lifecycle. The CIP does this by applying consistent processes to discover and validate operational strengths, innovations, and areas for improvement. CIP supports Agency leadership and program offices in issue resolution, improvement evaluation, and dissemination of potential best practices and innovations derived from disaster operations and exercises. CIP serves as a collaborative, agency partner focused on helping program offices in the field, Regions, and HQ continuously improve toward outcome-based change that saves lives, reduces risk, and reduces the complexity of FEMA. CIP is focused agency-wide

on disaster-related incidents and exercises.

1.2 Objective
The objective of this PWS is to outline the requirements and deliverables necessary to support the National Preparedness Assessment Division (NPAD) in preparedness analytics, assessment, evaluation, and reporting efforts.

NPAD accomplishes the mission through the following objectives that the products and services described in the Scope and Tasks support:

- **Assessing Whole Community preparedness** – Qualitative and quantitative assessment of the core capabilities in the National Preparedness Goal for the Whole Community: Federal, state, local, tribal, and territorial governments, private sector, non-government organizations, faith-based and community- based organizations and the American public.

- **Developing tiered disaster resilience and preparedness assessments and analytical, methodologies** – Developing tiered assessment products and methodologies that measure risk, capacities, and capability across the nation, including analyzing the targets, accomplishments, and gaps for hazards and threats, exposure, and vulnerability, including within the core capabilities of the Goal and the programs that support accomplishment of the Goal.

- **Developing standardized methods of disaster resilience and preparedness data collection and assessment** – Standardizing data collection methods and assessment methodology ensures consistency in the use and application of datasets to inform assessments of gaps and capabilities. This includes determining necessary data, identifying data sources, continually reviewing, and updating sources, and identifying and addressing gaps in data collection. Additionally, collaborating with stakeholders to develop data or sources that is not currently collected.

- **Assessing and evaluating the effectiveness of FEMA programs to enhance disaster resilience, including improving national preparedness** – Analyzing and evaluating the effectiveness of programs.

- **Leading Continuous Improvement and Innovation** - Providing insights from past disasters to improve future operations and supporting Agency program's efforts to evaluate and enhance delivery of assistance.

- **Developing and delivering products to shape strategic investments, future activities, and informed decisions to enhance national disaster resilience** – Drafting written and visual products that communicate disaster resilience, national preparedness, program effectiveness, and continuous improvement trends to stakeholders throughout the Whole Community.

1.3 Applicable Documents

The below listed laws and regulations are provided as references for this PWS. Nothing in the PWS supersedes applicable laws and regulations unless a specific exemption has been obtained. For clarification on case-by-case ambiguities, the contractor shall consult the COR.

- Post-Katrina Emergency Management Reform Act of 2006
- Disaster Recovery Reform Act of October 5, 2018
- Presidential Policy Directive / PPD-8: National Preparedness
- Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection
- 9/11 Commission Act of 2007
- Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
- Government Performance and Results Act (GPRA) Modernization Act of 2010
- Foundations for Evidence-Based Policymaking Act of 2018 ("Evidence Act")

1.3.1 Reference Documents

The following publicly available documents may be helpful to the Contractor in performing the work described in this document:

1.3.1.1 National Preparedness Goal, 2nd edition (NPG)
1.3.1.2 National Preparedness Report (NPR)
1.3.1.3 National Preparedness System
1.3.1.4 National Prevention Framework
1.3.1.5 National Protection Framework
1.3.1.6 National Mitigation Framework
1.3.1.7 National Response Framework (NRF)
1.3.1.8 National Disaster Recovery Framework
1.3.1.9 National Incident Management System (NIMS)
1.3.1.10 Comprehensive Preparedness Guide (CPG) 201
1.3.1.11 Comprehensive Preparedness Guide (CPG) 101
1.3.1.12 FEMA Strategic Plan
1.3.1.13 FEMA Directive (FD) 107-1 Continuous Improvement Program
1.3.1.14 National Threat and Hazard Identification and Risk Assessment Overview and Methodology

2.0 SPECIFIC REQUIREMENT/TASK AND DELIVERABLES

Specific Tasks are organized into similar categories. The contractor is required to perform at a minimum the following:

2.1 Data Collection Development and Management. This task supports the collection of qualitative and quantitative data through multiple methods for the development of disaster resilience and preparedness assessments, continuous improvement reports, and other products, as necessary.

The contractor shall:

- Manage the collection of disaster resilience data, including preparedness data, from both Federal and State, Local, Tribes, and Territories (SLTT) sources to inform annual assessments of capability and risk; assessments of disaster operations; and other indicators as required.
- Conduct rigorous data quality assessments that adhere to best practices in data quality assessment and data management.
- Analyze data sources, identify data gaps, recommend alternative data sources, and develop collection strategies to improve data quality. Develop feedback tools for partner organization's input to improve data collection approaches.
- Manage data in approved FEMA systems; code and categorize data using approved taxonomies. Support the modification and improvement of data management tools as required.
- Assist in the development of tools and platforms that internal and external stakeholders can use to access, explore, and analyze disaster resilience data, including threat, hazard, and capability data; exposure data; vulnerability data; operational data; and data on lessons learned from past disasters.

2.2 Research and Analysis This task concerns the analysis of data collected under task 2.1; it requires the use of quantitative and qualitative analytical capabilities in order to conduct analyses.

The contractor shall:

- In support of National Preparedness assessments and evaluations of National capability and risk, draft and maintain a FEMA-approved methodology to analyze disaster resilience, and preparedness information from the Whole Community. Apply the methodology to collected data and assess the current state, existing gaps, and direction of disaster resilience and preparedness.
- Develop research methodologies that support the sustained collection of information on priority topic areas across all disasters in a given year(s) using the National Collection Analysis Priorities; assist in analyzing all collected information, developing quarterly briefings, developing data visualization tools, and preparing end of year summary reports.
- Apply industry-standard and innovative qualitative and quantitative data analysis approaches that produce outputs that include data visualization and graphics.

2.3 Product Development - This task supports the above objectives to develop and deliver program specific products that shape strategic investments, future activities, and inform decisions. Tasks noted in this section support the table of deliverables found in section 2.8, and others identified during execution.

The contractor shall:

- Produce assessment reports, trend analyses, and cases studies pertaining to disaster resilience, and National Preparedness based on the data collection, research, and analysis tasks articulated above.
- Assist in the production of materials supporting these reports such as briefings, engagement materials, fact sheets, and talking points in accordance with appropriate FEMA and DHS style guides and templates.
- Identify and report on trends as identified in disaster resilience and preparedness products; track progress towards meeting identified targets as required, that includes whole community preparedness, program performance, disaster resilience, and preparedness investments.
- Develop executive summaries, synthesize findings, and support the development of new preparedness products in response to requests from internal and external stakeholders.
- Support the development of templates and resources in support of the National Continuous Improvement Guidance and develop topic-focused learning from past events for use by external partners.
- Develop knowledge summaries for external audiences learning from publicly available disaster and disaster resilience information.
- Assist in product concurrence and comment adjudication.

2.4 Training and Technical Assistance: These tasks concern the development and delivery of materials needed to assist program stakeholders with conducting disaster resilience and preparedness assessment activities, analyzing processes, and applying findings.

The contractor shall:

- Provide technical assistance and support to individual customers – Federal and SLTT stakeholders – including managing system helpdesk, user access and providing technical advice, process development, and expert knowledge of system and requirements.
    - Support technical assistance deliveries to whole community stakeholders on continuous improvement processes, which may cover topics such as implementing and managing a continuous improvement program, corrective action development and management, and using the continuous improvement process to support other preparedness activities.

2.5 Stakeholder Engagement and Outreach - This task ensures that products hat inform work across the agency, interagency, and with SLTT and private sector partners are effectively coordinated with stakeholders.

The contractor shall:

- Assist in developing and publicizing outreach documents, products, and content within FEMA or across the whole community using multiple mediums in coordination with FEMA's Office of External Affairs.

- Collect input on methodology, data collection, technical assistance, and outreach and engagement efforts from Federal, state, and local stakeholders, present findings, and develop recommendations to address input; support efforts to improve each of these areas.

2.6 Web Services and System Support – This task supports the objectives outlined above by developing tiered disaster resilience, and preparedness assessment, analytical methodologies, and standardized methods of data collection and assessment.

The contractor shall:

- Assist in defining functional requirements for FEMA systems that may be used to collect continuous improvement program information, as well as systems that may be used solely by NPAD.
- Provide technical support and training for stakeholders on data collection systems, including the development of user guides.
- Support development, implementation, tracking, testing, and evaluation of system development/maintenance requirements as part of the Continuous Improvement Information System.
- Provide user acceptance testing, develop user job aids and training, and support the user experience rollout, engagement, and ongoing management of user support.
- Support the transition of data from the Comprehensive After-Action Report Analysis Tool (CAARAT) into the Continuous Improvement Information System (CIIS). Support the continued development of modules in the CIIS, that may include the design and requirements identification, system development, system and user acceptance testing, system production, troubleshooting and system fixes, and the project and program management.
- Support data management and year-to-year continuity, including but not exclusive to import, export, and analytic functionality.
- Conduct data analysis of assessment system data to support the development of requirements for other IT initiatives.
- Prepare datasets and develop dashboards, as needed, for display on websites.

2.7 Contract Program Management: This task includes all activities of managing contractor work in support of the Division.

The contractor shall:

- Develop a Quality Control Plan (QCP). At a minimum, the QCP shall include a self-inspection plan for documents, deliverables and processes, an internal staffing plan, and an outline of the procedures the contractor will use to maintain quality, timelines, and responsiveness.
- In coordination the NPAD COR, plan and conduct routine meetings (to review progress and status of activities). Each review shall provide insight into expenditures, staffing, progress, and risks to include project briefings addressing

cost/price, schedule, performance, and status of each key element of the PWS, noting any problems or risks and alternative and recommended solutions. Frequency of meetings is at the discretion of the government as communicated via the COR or designee.

- Ensure that materials needed for meetings/presentations are provided to Government participants two (2) business days prior to the meeting and that data presented at program reviews is current within not more than five (5) business days.
- Attend weekly meetings with NPAD Project Leads and provide status updates on all tasks.
- Provide detailed monthly reports NLT than the 15th of each month for the previous calendar month; that include a summary of key work performed by deliverable. Invoices will also be due NLT than the 15th of each month, and invoices will also be based on the calendar month and include segregated costs by task and by staff for the spend plan versus actual for that reporting period, as well as track the percent of hours expended each month and the hours remaining on the contract for that option period.

2.8 Contract Deliverables: The following table is a list of the deliverables expected for the contract. Additional deliverables consistent with the tasks and activities listed in Section 2 of the Scope of Work will be coordinated between the COR, Project Manager and Contractor.

Item	Deliverable/Event	Branch	X per year	Task Reference
1	Call Order Kickoff Meeting	Overall	1	2.8
2	Call Order Draft PMP	Overall	1	2.8
3	Call Order Final PMP	Overall	1	2.8
4	Call Order Quality Control Plan	Overall	1	2.8
5	Develop Communications Materials	Overall	1	2.8
6	Call Out Close Out	Overall	1	2.8
7	THIRA/SPR Data Validation and Analysis	AAB	4	2.2, 2.3, 2.5, 2.6, 2.7
8	Investment Strategy for National Preparedness	AAB	1 every 2 years (estimated)	2.3, 2.5, 2.6
9	National Stakeholder Preparedness Review	AAB	1	2.3, 2.5, 2.6
10	National Threat and Hazard Identification and Risk Assessment (NTHIRA)	AAB	1 every 3 years (estimated)	2.3, 2.5, 2.6
11	National Preparedness Report (NPR)	AAB	1	2.2, 2.3, 2.5, 2.6
12	Annual Unified Reporting Tool (URT) Requirements Development	AAB	1	2.2, 2.3, 2.4, 2.5, 2.6, 2.7

13	THIRA Technical Assistance Virtual Sessions	AAB	10-12 sessions of 1-3 hours	2.4, 2.5, 2.6, 2.7
14	THIRA Technical Assistance In-person Sessions	AAB	3 sessions of 5 days (estimated)	2.4, 2.5, 2.6, 2.7
15	Steady State Community Profiles	AAB	6 (estimated)	2.2, 2.3, 2.4, 2.5, 2.6
16	Preparedness Capability Assessment	AAB	10 (estimated)	2.2, 2.3, 2.5
17	THIRA/SPR Data Analysis Tool (DAT) Development	AAB	3	2.4, 2.7
18	THIRA/SPR Dashboard	AAB	2	2.7
19	URT Support Calls	AAB	~26 (plus more if needed)	2.7
20	FEMA SPR Helpdesk (THIRA/SPR)	AAB	Year-round	2.7
21	THIRA/SPR Methodology Updates	AAB	1 every 3 years	2.2, 2.3, 2.5, 2.6
22	Online URT Maintenance	AAB	Year-round	2.7
23	National Collection Analysis Priorities (NCAP) Methodologies	CIIB	1	2.2, 2.3, 2.5, 2.6
24	NCAP Quarterly Briefs	CIIB	4	2.2, 2.3, 2.5
25	CAARAT Updates, biweekly	CIIB	26	2.7

3.0 Key Personnel

Key Personnel: Before replacing any individual designated as Key by the Government, the Contractor shall notify the Contracting Officer Representative (COR) no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the Key person being replaced, unless otherwise approved by the COR. The Contractor shall not replace Key Contractor personnel without approval from the COR.

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

- Contract Program Manager
- Continuous Improvement Integration Branch Lead
- Assessments and Analytics Branch Leads (2)
- Data Scientist
- THIRA and SPR Help Desk Support

Note: The Government may designate additional Contractor personnel as Key at the time of award as proposed by the offeror and accepted by the Government.

Program Manager: The Contractor shall provide a Program Manager who shall be responsible for all Contractor work performed under this PWS. It is anticipated that the Program Manager shall be a senior level employee provided by the Contractor. The name of the Program Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Program Manager, shall be provided to the Government as part of the Contractor's proposal. To be considered for the position, the Program Manager must have the following:

- Minimum of 10 years recent experience managing contracts or projects of similar size and scope.
- Federal, state and/or local Emergency Management Experience required
- Demonstrated ability to manage multiple complexes, time-critical support activities, including analysis and data collection.
- Outstanding written and oral communication skills.
- Ability to anticipate support needs in order to develop and execute detailed project work plans for addressing those needs.
- Master's Degree Required.

Branch Task Lead(s) The Contractor shall provide Leads for each branch who shall be responsible for all Contractor work assigned to their specific branch and performed under this PWS. The Branch Leads shall be a single point of contact for the Program Office leads. The names of any alternate(s) who shall act for the Contractor in the absence of the Branch Leads, shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the Branch Leads without prior approval from the Program and COR. Leads are branch specific and the qualification of each position is broken down below.

To be considered for the position, the Continuous Improvement Integration Branch Lead must have the following:

- Minimum of eight years recent experience managing contracts or projects of similar size and scope.
- Federal, state, and/or local Emergency Management Experience required.
- Disaster field experience preferred.
- Demonstrated ability to manage multiple complexes, time-critical support activities, including analysis and data collection.
- Outstanding written and oral communication skills.
- Ability to anticipate support needs in order to develop and execute detailed project work plans for addressing those needs.
- Undergraduate Degree Required.

To be considered for the position, the Assessment and Analytics Branch Leads (2) must have the following:

- Minimum of eight years recent experience managing a contract of similar size and scope.
- Federal, state, and/or local Emergency Management Experience required.
- State and local Emergency Management Experience required.
- Demonstrated ability to manage multiple complexes, time-critical support activities, including analysis and data collection.
- Outstanding written and oral communication skills.
- Ability to anticipate support needs in order to develop and execute detailed project work plans for addressing those needs.
- Master's degree required.

Data Scientist: The Contractor will provide a Data Scientist to support the work of the Measures and Standards and Assessments and Analytics Branches on a full-time basis. The names of any alternate(s) who shall act for the Contractor in the absence of the Data Scientist, shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the Data Scientist without prior approval from the Program and COR. The qualifications for the Data Scientist shall include:

- Demonstrated ability to manage multiple complexes, time-critical support activities, including analysis and data collection.
- Master's and 3 years of experience or equivalent
- Outstanding written and oral communication skills.
- Significant coursework or training in statistics (at least three courses beyond introductory statistics), including hypothesis testing, linear regression modeling, data entry, data cleaning, data wrangling, familiarity with assumptions and use- cases for various clustering tasks, classification algorithms, and non-regression modeling tasks. Graduate-level education preferred.
- Demonstrated experience using Government-owned administrative or survey data to perform advanced hypothesis testing, linear regression modeling, and other statistical analyses.
- Access to and experience with R, Python, SPSS, or Stata statistical software.
- Experience with large datasets preferred.

3. THIRA and SPR Help Desk Support: The Contractor will provide a Help Desk Support lead to provide customer service and support related to the THIRA/SPR assessment and online URT on a full-time basis. The Help Desk support team member will monitor the FEMA-SPR email inbox and customer support phoneline. The help desk is a year-round service that is provided to the community and is often the first contact AAB has with SLTT partners. The names of any alternate(s) who shall act for the Contractor in the absence of the Help Desk Support team member, shall be provided to the Government as part of the Contractor's proposal. Additionally, the Contractor shall not replace the Help Desk Support member without prior approval

from the Program and COR. The qualifications for the THIRA and SPR Help Desk Support shall include:

- Minimum of two years recent, similar project experience.
- Bachelor's degree required.
- Outstanding written and oral communication skills.
- Demonstrated ability to manage multiple, time-critical support activities simultaneously.
- Ability to anticipate support needs in order to provide efficient and effective customer service to individual customers, as well to program leads

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

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

3.2 Removing Employees for Misconduct or Security Reasons: The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

4.0 OTHER APPLICABLE CONDITIONS

4.1 Security

Contractor access to classified information is not currently required under this PWS.

4.1.1 Standard Security Language

BACKGROUND INVESTIGATIONS

All contractor personnel who require access to DHS or FEMA information

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

Low Risk without Information System Access

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

Low Risk with Information System Access

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

Moderate Risk

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

High Risk

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

Background Investigation Process

To initiate the request to process contractor personnel, the Contractor shall provide the FEMA Contracting Officer's Representative (COR) with all required information and comply with all necessary instructions to complete Section II of the FEMA Form 121-3-1-6, "Contract Fitness/Security Screening

Request." The FEMA COR shall ensure that all other applicable sections of the FEMA Form 121-3-1-6 are complete prior to submitting the form to FEMA PSD for processing. The Contractor shall also provide the FEMA COR with completed OF 306, "Declaration for Federal Employment," forms for all contractor personnel.

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

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

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

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

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

FEMA PSD will only accept complete packages consisting of all 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 have any right to such a grant of temporary eligibility. The grant of such temporary eligibility shall not be considered as assurance that the contactor personnel will remain eligible to perform work under this contract upon completion of and final adjudication of the full background investigation.

Upon favorable adjudication of the full background investigation, FEMA's Personnel Security Division will update the contractor personnel's security file and take no further action. In any instance where the final adjudication results in an unfavorable determination FEMA's Personnel Security Division will notify the contractor personnel directly, in writing, of the decision and will provide the COR with the name(s) of the contractor personnel whose adjudication was unfavorable. The COR will then forward that information to the Contractor. Contractor personnel who receive an unfavorable adjudication shall be ineligible to perform work under this contract. Unfavorable adjudications are final and not subject to review or appeal.

Continued Eligibility and Reinvestigation

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

Exclusion by Contracting Officer

The Contracting Officer, independent of FEMA's Personnel Security Division, may direct the Contractor be excluded from working on this contract. Any contractor found or deemed to be unfit or whose continued employment on the

contract is deemed contrary to the public interest or inconsistent with the best interest of the agency may be removed.

FACILITY ACCESS

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

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

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

The Contractor shall notify the FEMA COR of all terminations/resignations within 48 hours 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.

SECURITY TRAINING

SECURITY:

Contractor access to unclassified, but Security Sensitive Information may be required under this PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

Unauthorized Disclosure of Classified or Unclassified Information

Contractors and subcontractors who are working on this contract shall receive Unauthorized Disclosure of Classified or Unclassified Information training. Access to the training can be obtained at:
https://securityawareness.usalearning.gov/disclosure/index.html

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
https://securityawareness.usalearning.gov/opsec/

Insider Threat Training

Insider Threat training for contractors can be found at:
https://securityawareness.usalearning.gov/itawareness/index.htm#

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 shall:

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.

Standard Training Language – Unauthorized Disclosure of Classified or Unclassified Information

All contractors and subcontractors are required to train on Unauthorized Disclosure of Classified or Unclassified Information to perform duties established by the Government during the performance period of and execution of this contract.

Access to the training can be obtained at:
https://securityawareness.usalearning.gov/unauthorizedrefresher/index.htm

Certificate of completion should be kept on hand by contractor and provided upon request to the FEMA Contracting Officer Representative within 24 hours

4.2 Period of Performance

The period of performance for this contract is a one-year base period with four one-year option periods as follows:

Base Period	09/02/2021 – 09/01/2022
Option Period One	09/02/2022 – 09/01/2023
Option Period Two	09/02/2023 – 09/01/2024
Option Period Three	09/02/2024 – 09/01/2025
Option Period Four	09/02/2025 – 09/01/2026

4.3 Place of Performance

The primary place of performance will be a combination of the Contractor's facilities, designated alternate work location, and DHS/FEMA at 400 C Street SW Washington DC 20472. All contractors are subject to the standard remote work polices and guidelines that apply to federal employees this includes any policies or

guidelines adjusted for incidents such as COVID that require remote work. Contractors shall follow procedures for federal employees.

4.4 Hours of Operation

Contractor employees shall generally perform all work between the hours of 8:00am and 5:00pm EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this PWS.

4.5 Travel

Contractor travel shall be required to support this requirement. All travel required by the Government outside a 50 miles radius will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event. Payable under travel CLIN line in contract.

4.6 Post Award Conference

The Contractor *shall* attend a Post Award Conference with the Contracting Officer and the COR five – ten business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held at the Government's facility, located at 400 C ST SW Washington, DC or via teleconference.

4.7 Project Plan

The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 10 business days after the Post Award Conference.

4.8 General Report Requirements

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows and Microsoft Office Applications).

4.9 Intellectual Property/Rights in Data

In accordance with Federal Acquisition Regulation (FAR) 52.227-14, Rights in Data – General, the Government shall have unlimited rights in data first produced

in performance with this contract and data delivered under this contract. All intellectual property generated and/or delivered pursuant to this Statement of Work will be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with government funds, a nonexclusive "paid-up" license to practice any patentable invention or discovery made during the performance of the Contract, and a "paid-up" nonexclusive and irrevocable worldwide license to reproduce all works (including technical and scientific articles) produced during the Contract.

4.10 Protection of Information

Contractor access to information protected under the Privacy Act may be required under this PWS. Contractor employees shall safeguard this information, as well as all data provided by Federal and STTL agencies and stakeholders, and pre-decisional analyses, against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

Contractor access to proprietary information is required under this PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

4.11 Section 508 Compliance Requirements

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div
5. 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.

4.12 Section 508 Requirements for Technology Services

1. When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution, or replacement. The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed upgrades, substitutions, and replacements prior to acceptance. The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.2 508 (or successor versions). The template can be located at https://www.itic.org/policy/accessibility/vpat

2. When providing Platform as a Service (PaaS) or Software as a Service (SaaS), the contractor shall ensure services conform to the applicable Section 508 standards (including the requirements in Chapter 5 for software and WCAG Level A and AA Level 2.0 success criteria for web and software. When the requirements in Chapter 5 do not address one or more software functions, the Contractor shall ensure conformance to the Functional Performance Criteria specified in Chapter 3.) The agency reserves the right to request an Accessibility Conformance Report (ACR) for PaaS and SaaS offerings. The ACR should be created using the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be located at https://www.itic.org/policy/accessibility/vpat

3. When providing cloud hosting services (Infrastructure as a Service, Platform as a Service, Software as a Service, etc.) the Contractor shall ensure user administrative screens, dashboards and portals used to configure, and monitor cloud services conform to the Section 508 standards.

4. The Contractor shall ensure cloud hosting services shall not reduce the level of Section 508 conformance for ICT migrated by DHS to the cloud hosting environment.

5. 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.

6. 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.

7. 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.

8. 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

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

4.13 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

4.14 Section 504 Requirements

The Contractor/Provider shall comply fully with Section 504 of the Rehabilitation Act of 1973, as amended, which prohibits discrimination against qualified individuals with disabilities. No otherwise qualified individual with a disability shall, solely by reason of his or her disability, be excluded from participation in, be denied the benefits of, or subjected to discrimination under any program or activity for which the Contractor/Provider is awarded a contract and/or receives federal financial assistance from the Federal Emergency Management Agency. This includes, but is not limited to, providing reasonable accommodations and modifications to ensure effective communication access, physical access, and program access to all participants, including persons with disabilities. The Contractor/Provider shall incorporate this language in any subcontracts related to the provision of the FEMA public-facing program or activity.

5.0 GOVERNMENT FURNISHED RESOURCES

The Government will provide the workspace, equipment and supplies necessary to perform the on-site portion of Contractor services required in this contract, unless specifically stated otherwise in this work statement.

The Government will provide all necessary information, data, and documents to the Contractor for work required under this contract.

The Contractor shall use Government furnished information, data, and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data, and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data, and documents to outside parties without the prior and explicit consent of the Contracting Officer.

6.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment, and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified.

7.0 GOVERNMENT ACCEPTANCE PERIOD

The COR or designee will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR or designees will send an e-mail to the Contractor POC notifying it that the deliverable has been accepted.

7.1 The COR or designee will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR or designee of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

7.2 The COR will have 10 business days to review deliverables and make comments. The Contractor shall have 5 business days to make corrections and redeliver.

7.3 All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

8.0 PERFORMANCE REQUIREMENTS SUMMARY (PRS)

The PRS establishes key elements of Contractor performance that represent "mission essential" service requirements, which are identified in the table below. The performance objective or "standard" describes the minimum acceptable level of service by the Contractor for satisfactory performance. The "Acceptable Quality

Level (AQL)" column displays the required level of performance, which, if not met, evokes the negative incentive specified in the table below.

The Quality Assurance Surveillance Plan (QASP) outlines how FEMA intends to evaluate the contractor's performance.

Desired Output	Performance Standard	Acceptable Quality Level (AQL)	Monitoring Method	Performance Incentive / Disincentive
Deliverables submitted on time	Deliverables submitted on or before due dates without reminders from FEMA	98%	Task Lead, COR and/or designee monitor due dates and notes when deliverables are submitted / completed	**Incentive**: COR will document performance via CPARS official government system of record for contractor performance **Disincentive**: COR will document performance via CPARS official government system of record for contractor performance
Monthly and as needed progress reports to document ongoing activities	Accurate and complete reports by the 15th of every month. On a monthly basis, the Contractor provides a review of contract performance to communicate Task achievements, progress to date, and identified performance risks.	98%	Task Lead, COR, or designee reviews submitted reports for accuracy, completeness, and quality	
High quality deliverables	Deliverables submitted that meet or exceed requirements and support objectives of PWS. Deliverables do not require significant rework before	95%	Task Lead, COR or designee review submitted deliverables and measures quality against standards in PWS, awarded contract, Quality Control Plan	
	being accepted by the government		(QCP) and project plan as appropriate.	
Deliverables formatted	Continuous Improvement	98%	Task Lead, COR, or designee	

correctly and without grammatical and punctuation errors	Program Style Guide and commonly accepted grammar and punctuation styles and standards, like APA, MLA and/or Chicago.		review submitted deliverables against Style Guide and applicable style requirements. Grammar Rules, Formatting, and Protocols of Standard Written English apply.	

9.0 PRIVACY CLAUSES

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

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

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107- 296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

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

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII

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

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

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

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

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

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

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

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

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

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

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy

Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

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

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

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

(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:

(3) 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.

(4) 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.

(5) *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.

(6) *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.

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

(f) *Sensitive Information Incident Reporting Requirements.*

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

failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

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

(g) *Sensitive Information Incident Response Requirements.*

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

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

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

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

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

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

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

utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or 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.*

(end of clause)

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

Security Training Requirements.

All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwisespecified, 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.

(end of clause)

Prior to any access, collection, maintenance, dissemination, or use of PII (as defined in DHS policy) by the contractor and prior to any access to FEMA systems to conduct the work identified in this contract, the COR and contractor, in consultation with the FEMA Privacy Office, will complete an Information Sharing and Access Agreement (if necessary) and obtain an adjudicated PTA (as well as PIA and SORN coverage where applicable) that addresses privacy compliance coverage for the IT systems from which data is obtained and coverage for the program the contractor's work is supporting.