PERFORMANCE WORK STATEMENT

Department of Homeland Security

Federal Emergency Management Agency

Regional Support for Individuals and Community Preparedness and Outreach

(2-17-2023)

Table of Contents

A. Purpose

Presidential Policy Directive-8 (PPD-8): National Preparedness tasked the Secretary of Homeland Security with coordinating "a comprehensive campaign to build and sustain national preparedness, including public outreach and community-based and private sector programs, to enhance national resilience, the provision of Federal financial assistance, preparedness efforts by the Federal Government, and national research and development efforts."

The U.S. Department of Homeland Security (DHS), Federal Emergency Management Agency (FEMA), Individual and Community Preparedness Division (ICPD) has requirements for program support; regional support; research, analysis, and evaluation; and outreach and communication services to support FEMA mission to increase individual, and community preparedness and resiliency.

ICPD supports survivors and communities by building the capabilities of individuals and families to be aware of and prepared for the hazards they face. ICPD programs empower U.S. residents to become active participants in community resilience, in support of FEMA's strategic priorities. ICPD's research informs actions taken by individuals and communities across the nation to stay safe before, during, and after a disaster.

ICPD's goal is to achieve a culture of preparedness for the U.S population of over 322 million. Success is a culture where preparedness is part of everyday life: Americans know their relevant hazards and have taken actions to prepare themselves. Together, the whole community works to plan for and practice the community's response to both likely and unexpected hazards.

In order to achieve its mission, ICPD has numerous programs and key initiatives focused on communicating protective action guidance and tools to the general public. Work under this task will provide direct support to FEMA Regions for these programs, advancing their effectiveness in order to create a culture of preparedness in America.

B. Background

Preparedness begins with the individual. FEMA's Individual and Community Preparedness Division serves as the main preparedness link to individuals and families. ICPD connects individuals, organizations, and communities with research and tools to build and sustain capabilities to prepare for any disaster or emergency.

The science supporting FEMA's individual and community preparedness programming includes the National Household Survey (NHS) and protective actions guidance. The NHS, implemented annually since 2013, provides insight into people's preparedness attitudes, beliefs, behaviors, and actions. Findings from the NHS help to refine and improve the Agency's engagement and

capacity building strategies for individuals and communities. ICPD provides the public with current, research-validated guidance (e.g., drop, cover, and hold on for earthquakes; run, hide, fight for active shooters; etc.) so that they may employ these protective actions to protect themselves from threats and hazards, and ultimately save lives. This research enables FEMA to better understand effective preparedness actions and ways to motivate the public to take those actions. FEMA also conducts research to understand and improve how underserved communities receive critical preparedness information and strategies to help them take steps to prepare themselves, their families, and their communities. Results from this effort can help to modify and improve how the Agency communicates and collaborates with underserved populations, potentially saving lives in communities disproportionately affected by disasters.

C. Scope

The scope of this requirement includes Preparedness and Outreach and Administration and Management Support.

The Contractor shall provide regional support for Individual and Community Preparedness and Outreach. The Contractor shall provide regional support by providing Regional Preparedness Liaisons (RPLs). RPLs, also known as Subject Matter Experts (SME) and Business Specialist shall provide technical assistance and program support to FEMA Regions and partners, typically supporting more than 600 preparedness events across the nation annually. In addition, RPLs provide program support for regional programs that fall under the mission of the FEMA ICPD

The Contractor shall provide Administrative and Management support to ensure efficient communication and operations in operation of this this task order. Specifically, the contractor shall provide a Program Manager for this project to manage day-to-day operations as well as strategic planning.

D. Performance Summary Requirement (PSR)

This requirement includes a Performance Requirements Summary (PRS). The PRS plays an integral role in the administration of the task order. In addition to any applicable inspection clauses or other related terms and conditions contained in the task order award the PRS shall serve as a primary tool for inspection and acceptance of services as facilitated by the COR. Evaluation of the Contractor's overall performance shall be in accordance with the performance standards set forth in the PRS, and will be conducted by the COR. The PRS constitutes a material aspect of the task order and will not be changed or otherwise modified without prior written approval of the Contracting Officer.

All work products and deliverables shall, at a minimum, be 95% free of errors, specifically content, spelling, grammar, formatting, and punctuation.

Written documents shall be concise and clearly written. The Contractor shall ensure the accuracy, functionality, completeness, professional quality, and overall compliance with government guidelines/requirements of the deliverables.

The PSR is included within Attachment 1, Quality Assurance Surveillance Plan (QASP)

E. Specific Mandatory Tasks and Associated Deliverables

The work described herein is divided into two task areas: Task 1, Regional Preparedness and Outreach Support and Task 2, Administration and Management Support.

Task 1: Regional Preparedness Outreach and Support

A. Regional Preparedness Liaisons

The contractor shall provide 9 Regional Preparedness Liaisons (RPLs) which shall be physically located within the following FEMA Regions:

- Region 1 (Boston, MA)
- Region 2 (New York, NY)
- Region 3 (Philadelphia, PA)
- Region 4 (Atlanta, GA)
- Region 5 (Chicago, IL)
- Region 7 (Kansas City, MO)
- Region 8 (Denver, CO)
- Region 9 (Oakland, CA)
- Region 10 (Bothell, WA)

*Note: Region 6 will not have an RPL.

RPLs shall serve as both Emergency Preparedness Program Specialist/Subject Matter Experts (SMEs) as well as a Business Specialists. RPLs shall support the preparedness efforts of FEMA region through participating in bi- monthly conference calls with all regions and preparing minutes; supporting regional meeting(s); developing PowerPoints and materials for regional meetings and conferences; and supporting regional communications with state leadership, to include conference calls, and regional pilot projects.

Regional support shall accommodate individual regional needs or priorities as directed by the regional Community Preparedness Officer (CPO) or other regional leadership. The RPLs may also support other activities including, but not limited to:

- eBrief Newsletters. Research, write, and format electronic newsletters for preparedness focus areas, including Community Emergency Response Team (CERT), Youth, and other topics. All writing shall be free of grammatical errors and comply with DHS writing standards. Digital contact lists will be maintained to ensure accurate points of contact.
- Social Media. Develop and execute a social media strategy, as requested, to increase presence of ICPD and FEMA social media handles and hashtag topics including partnerships with other agencies and partners. Social media searches and reports for preparedness programs (i.e., CERT and Citizen Corps) will be developed during preparedness events and/or initiatives and disasters to highlight program connections in the community.
- Webinars. In coordination with the appropriate program leads, develop annual webinar schedule, including timeframes, topics, and potential participants. Host webinars on

specific ICPD topics. Support includes recommended webinar topics, identifying guest speakers, support for presentations, operating webinar software, and managing the webinar event, including participant Q&A, and administrative follow-up.

- Mailbox Inquiries. Support for managing and responding to inquiries from the public, including follow-up communication with appropriate federal staff where decision points are required.
- Discussion Boards. Website discussion boards allow for open discussion of preparedness topics with participants from around the country. The contractor shall provide support for managing content of topical website discussion boards and identify trends in topics discussed on FEMA preparedness websites.
- Child Safeguarding. Provide subject matter expertise and support in Child Safeguarding and develop/update/maintain guidance as well as provide training as/if needed. In addition, the contractor shall serve as a consultant for ensuring that programs and products observe or integrate child safeguarding principles and best practices.

RPLs shall work with the regions to identify collaboration opportunities and identify potential demographics that may benefit from added focus. Once identified, the RPLs shall work with the regions to create a *Regional Engagement Strategy* to be submitted within one (1) month of the beginning of the period of performance and annually thereafter.

The contractor shall support individual and community preparedness throughout the Region and work directly with the state and local partners to help implement regional goals and objectives and promote FEMA and approved partner preparedness programs to enhance individual, organizational, and whole community preparedness. RPLs shall assist the delivery of community preparedness events within their regions as well as national level initiatives.

Preparedness events may include, but are not limited to:

- You Are the Help Until Help Arrives training delivery
- National, Regional, State, Tribal, and local Youth Preparedness Council recruitment, outreach, and coordination
- Ready Business and Organization Preparing for Emergency Needs (OPEN) preparedness workshops
- Community preparedness events
- Ready Campus preparedness workshops
- Community preparedness and education outreach events
- FEMA Regional preparedness communication content creation, maintenance, and promotion, such as via social media and releases.

RPLs shall provide a written After-Action Report (AAR) to ICPD and the Region POC within five (5) business days of completion of a preparedness event that outlines the perceived problem of the requestor, describes the support provided, and identifies the problems encountered or unanticipated circumstances. The AAR shall include:

- Names and titles of personnel participating (contractor and requestor); Detailed overview of service provided;

- Number of support hours provided; support provider issues or concerns;
- Event data analysis (trends, shortfalls, etc.)
- Identified best practices and recommendations to resolve problems and improve future support for events; and
- Summary of additional ODCs to include travel and printing as well as any pending follow-up items identified during or after support delivery.

RPLs shall be identified as contractors performing in support of FEMA preparedness; perception that RPLs are Government employees is strictly prohibited.

During times of disaster, RPLs may also be asked to shift their focus and support to meet increased demands related to the above work in support of ICPD or Region efforts. Specifically, RPLs may be asked to adjust their hours of operation or travel to other regions to provide additional support. The RPL shall provide assistance as directed by ICPD or regional leadership.

Task Deliverables:

Deliverable 1. A.1 Regional Engagement Strategy [within one (1) month of the start of the performance period, then yearly]

Deliverable 1. A.2 After Action Reports [within 10 business days of preparedness event]

B. Preparedness Headquarters Support

The contractor shall provide preparedness support for ICPD at FEMA headquarters and shall have at least one contractor (to include the program manager at a minimum) on-site in the Washington, DC headquarters office.

The contractor shall provide a consolidated quarterly Strategy Implementation Report that reviews and assess the implementation of each approved RPL strategy. At a minimum, this report shall identify strengths, challenges, and proposed solutions to overcome the identified challenges.

The contractor shall provide a monthly Regional Preparedness Activity Report. This report will identify RPL-supported activities and provide the following information, at a minimum, about the activities: location, organizations involved, number of participants, and a short description of the event and activities.

The contractor shall prepare a monthly Federal Preparedness Coordinators email for distribution by the ICPD Director to the or other regional leadership. These FPC emails provide high-level information about national preparedness activities and initiatives and often include announcements and reminders of activities and deadlines.

The contractor shall coordinate efforts across all regions to establish uniform, six-month preparedness goals that enable the contractor to obtain regional goal and alignment information from each of the regions. Subsequently, the contractor shall submit a Bi-Annual Regional Goals and Alignment Report provides national level analysis that, among other things, highlights trends and strengths and identifies possible gaps across nine Regions and FEMA headquarters.

The contractor shall also provide Bi-Annual Regional Collaboration Reports from each of the regions that lists all state, local, tribal, territorial, or regional collaborative activities related to preparedness programs and initiatives (e.g., Youth, CERT, or Until Help Arrives).

The contractor shall provide an Annual Collaboration Report that lists all state, local, tribal, territorial, or regional collaborative activities related to preparedness programs and initiatives (e.g., Youth, CERT, or Until Help Arrives). This report shall also provide an analysis of HQ, regional, and partner contributions for successful events. In addition, the report should provide recommendations for subsequent activities.

Task Deliverables:

Deliverable 1. B.1	***Strategy Implementation Report [quarterly]***
Deliverable 1. B.2	***Regional Preparedness Activity Report [5th business day of each month]***
Deliverable 1. B.3	***Monthly FPC Email [5th business day of each month]***
Deliverable 1. B.4	***Bi-Annual Regional Goals and Alignment Report [twice yearly]***
Deliverable 1. B.5	***Bi-Annual Regional Collaboration Report [twice yearly]***
Deliverable 1. B.6	***Annual Collaboration Report [yearly]***

C. Optional Headquarters Surge Support

On an optional basis, the Contractor may be required to provide additional surge support to meet greater than expected workload associated with this PWS. The requirement for surge support is most often associated with periods of increased ICPD-managed activities, such as the National Preparedness Month (September), hurricane season (spring-summer) and/or events such as the FEMA Youth Preparedness Council Summit (usually occurring in July). To support these periods of elevated activity, the Government anticipates a surge force capacity including program manager, subject matter expert, and business specialist (RPL) being required. While the exact timing and duration of this requirement cannot be determined at task order award, the Contractor shall offer surge support at a firm, fixed price as required by the Government. Specifically, up to four instances of the following may be exercised in each period of performance.

- Program Manager (Emergency Preparedness Coordinator) – 25 hours
- Emergency Preparedness Program Specialist (SME) – 25 hours
- Emergency Preparedness Specialist – 200 hours

Surge support tasks may also include, but is not limited to, the following:

- Assess current training materials (participant manual, instructor guide, slides, and AV content) and develop a project plan for updating for a virtual environment (note: instructor guide will need extensive updates for teaching virtually and students will need technical assistance info)
- Update training content based on government approval from the assessment
- Pilot the virtual training and collect feedback
- Recommend further updates based on participant feedback

- Update training based on government approval from feedback
- Publish new virtual training course on existing ICPD platforms (www.community.FEMA.govand/or ready.gov)
- Create a virtual training promotion plan that will encourage the public and stakeholders to leverage the new content (include social media, stakeholder engagement, webinars)
- Lead virtual instruction of each course, open to the public, at least 10 times, distributed across time zones
- Translate the new content into additional languages
    - The following is a prioritized list of courses for "virtual translation."
        - Student Tools for Emergency Planning (STEP)
        - Organizations Preparing for Emergency Needs (OPEN)
        - Emergency Financial First Aid Kit (EFFAK)
        - Ready 2 Help
        - You Are the Help Until Help Arrives
        - CERT Basic Training
        - CERT Supplemental
        - Ready Business (multiple hazards)
        - Virtual Preparedness Fair (including the basic Take Action messages such as completing a family communication plan)

For each instance of surge support, the Contractor shall provide a summary report of the activities and associated outcomes. The report shall be no more than two pages in length.

Specific Deliverables:

Deliverable 1. C.1 ***Surge Support Report [NTE Four Times Annually]***

D. Preparedness Summit Event Support

On an annual basis, the Contractor shall plan and execute a summit-type event for networking and collaboration among federal colleagues working in the individual and community preparedness space. The contractor shall support ICPD in the following areas:

- Logistical planning
- Attendee and speaker coordination and outreach
- Drafting materials including, but not limited to, agendas, memos, guides, and after-action reports
- Event management (note taking, audio/visual technical facilitation
- Administrative oversight to support the above.

RPLs working in the regions should plan to attend the event as participants, but should not be used for event planning or execution.

Timing for the event will likely coincide with another ICPD-hosted event, the annual Youth Preparedness Council Summit. As such, coordination with federal staff and other contract support staff will be required.

Deliverable 1. D.1 Preparedness Summit Event (Once Annually)

Task 2: Administration and Management

A. Project Management Plan (PMP)

The Contractor shall provide a detailed PMP with their proposal, which shall include the intended approach, work plan, and project schedule including deliverables, tasks, and subtasks, with major milestones. In addition, the PMP will include specific sections, identified below, which present the Contractor's PMP plan for completing the task order describing the technical approach, management plan, organizational structure and resources, and management controls that will meet the objectives of this PWS.

The Contractor's PMP shall be responsive to this PWS and describe, in further detail, the approach to be used for each aspect as defined in the proposal. The Contractor shall keep the PMP up to date throughout the period of performance; specifically, the vendor shall provide recommended updates in the form of tracked changes in Microsoft Word, on a monthly basis. Further, the Government may, at any time, request additional updates that shall be completed by the vendor and delivered to the Government no more than five (5) days after the request. These updates may include the identification of specific activities in support of the scope of work that could not be identified at the time of the initial plan, ensuring that the plan becomes more definitive as such activities become known.

The PMP shall include the following:

- Staffing & In-processing Plan: The staffing plan is to define the roles and responsibilities for all personnel supporting the task order. The goal of the plan is to ensure the task order support staff is properly aligned to the strategic goals, mission, and objectives of FEMA. Staffing plan shall also include the Contractor's organizational structure in support of the task order. The Contractor shall provide a detailed hiring plan and complete all contractor fitness forms. The Staffing Plan shall also demonstrate the Contractor's process for immediately identifying and taking appropriate remedial action in addressing Contractor personnel determined to be unacceptable in terms of technical competency or personal conduct in performance of contract activities. Contractor remedial actions shall be executed in a manner that does not disrupt or degrade the quality or timeliness of services. Only trained staff shall be permitted to work in support of this task order (see Training Plan, below, for more details). All variations must receive prior approval from the PM and COR. As a part of this plan, the Contractor shall create and maintain a staffing tracker. The tracker shall include issues related to hiring and also be included on the Risk Assessment and Mitigation Plan.
- Contractor Communication Plan: The Contractor shall outline the roles and responsibilities of the Contractor's project participants in the review, approval, and dissemination of information about key project processes, events, documents, and milestones.
- Risk Assessment and Mitigation Plan: The Contractor shall outline the plan to conduct risk identification, risk analysis, risk management, and risk monitoring and reporting,

focusing on the processes, resources, and data sources critical to managing the project. This plan shall provide the basis for the weekly reporting identified in in this document.

- Quality Control Plan (QCP): The QCP shall provide specifics regarding how the Contractor defines, implements, and assures quality and compliance to the Quality Assurance Surveillance Plan (QASP) during the task order life. The QCP shall be reviewed quarterly and if there are any changes, the updated QCP shall be submitted to the PM and COR. The QCP shall document the overall approach to quality assurance activities.
- Training Plan: Specific staff training requirements and qualifications have been defined within this document (e.g., Insider Threat, OPSEC). The Contractor shall outline a plan for how staff supporting these tasks will be trained according to these requirements.
- Transition-In Plan: The Contractor shall execute a transition to fully migrate support from the incumbent contractor by May 31, 2023, ensuring minimum disruption to Government business. The Contractor shall document a Transition-In Plan, including a schedule depicting the transition activities and milestones for accomplishing the transition in. The Transition-In Plan shall detail how the Contractor will establish procedures with the outgoing contractor to transition support while maintaining continuity of services with no degradation in service. This includes defining processes for turnover of system accounts, privileges, access, and administration.
- Transition-Out Plan: The Contractor shall document a Transition-Out Plan that describes the process, details, and schedule for providing an orderly transition during the Contract's phase out period in accordance with the PWS. An initial draft of this document shall be created along with the PMP and shall be updated 90 days prior to the end of the task order. The objectives of the Transition-Out Plan are to minimize the impacts on continuity of operations; maintain communication with staff and affected stakeholders; identify key issues; and overcome barriers to transition. The Contractor shall establish a transition management team capable of providing overall management and logistical support of all transition activities. The Contractor shall document within the Transition-Out Plan a proposed schedule for report status to the PM, COR, and CO and/or task order close-out meetings leading up to the end of the task order. The Transition-Out Plan shall include the following:
- Inventory all Government Furnished Equipment (GFE) and Government Furnished Information (GFI) in Contractor possession;
- Status of all deliverables, current issues, problems, or activities in process that require immediate action; and
- How the Contractor shall ensure proper transfer of GFE, GFI, and records and documents to the Government prior to the end of the period of performance.

Task Deliverables:

Deliverable 2. A.1 Project Management Plan (PMP) [Delivered at proposal, Reviewed at Kick-Off Briefing 5 business days after award]

Deliverable 2. A.2 Project Management Plan (PMP) Updates [NLT 5th business day of each month]

B. Project Kick-Off Briefing

The Contractor shall host a project Kick-Off Briefing with Government project team. The Kick-Off Briefing shall be held within five (5) business days after task order award or as agreed upon between FEMA Government project manager (PM), COR, and Contractor. At the Kick-Off Briefing, the Contractor shall brief the details of the Project Management Plan (PMP).

Task Deliverable:

Deliverable 2. B.1 ***Project Kickoff Briefing [5 business days after award]***

C. Monthly Interim Progress Review & Report

Monthly Interim Progress Review (IPR) activities shall support the Government in implementing disciplined, comprehensive, and flexible program and project management processes, including monitoring of project metrics; rigorous risk management; and prompt reporting on Government-approved schedule, performance, and risk baseline. The vendor shall provide a Monthly Status Report (MSR) to the Government, electronically, no later than the 5th business day of each month. This MSR shall cover all task order-related activity and any other information, as defined by the COR, for the previous month. For example, the MSR delivered on the 5th business day of November shall detail all activity occurring in October.

The MSR shall present the work to be accomplished during the subsequent month. This report shall also identify any problems that arose and a statement explaining how the problem was resolved. This report shall also identify any problems that have arisen but have not been completely resolved with an explanation. The MSR shall include, at a minimum, the following items, or characteristics:

- Be organized according to the tasks as described in this performance work statement (PWS)
- Roster of personnel
- Pending in-processing status for new personnel
- Planned travel for the upcoming 60-day period
- Planned absences for the upcoming 30-day period
- Current expenditures and forecasted expenditures for travel and printing, including Post-Trip Reports with a detailed breakdown of the actual expenditures invoiced, identification of project risks, a summary of the tasks and work products completed, and a status of all deliverables.

Task Deliverables:

Deliverable 2. C.1 ***Monthly Status Report [NLT 5th business day of each month]***

Deliverable 2. C.2 ***Monthly IPR Briefing (NLT 10th business day of each month]***

D. Weekly Status Report

The Weekly Status Report (WSR) shall highlight risks and issues as well as any outstanding items. Risks and issues shall be reported during the weekly update meetings as critical, high, medium, or low. A description shall be included of the risk/issue, the owner, progress made,

and management strategy as applicable. Weekly status shall be provided on each risk until they are closed out. The COR may request that a perceived risk or issue be added and tracked for the task order. The WSR shall be delivered via email to both the COR and PM.

Task Deliverables:

Deliverable 2. D.1 ***Weekly Status Report [Weekly - COB Mondays]***

E. Project Plans

The Contractor shall identify the milestones and task activity that will take place against all major project work. The Contractor shall provide resource and cost information (as applicable) as part of this plan. Draft Project Plans for program support, communication or evaluation are due within five (5) business days of receipt of the task by ICPD.

Task Deliverables:

Deliverable 2. E.1 ***Project Plans [within 5 business days of assignment]***

D. Administrative Tasks

The vendor shall complete standard administrative tasks (e.g., background investigation forms, staff roster, mandatory training) Project staff cannot start work on projects until the COR has received the fitness screening approval from FEMA personnel security.

Invoices must be submitted using SF 1034 and SF 1035. In addition, all invoices must include an Excel spreadsheet, with formulas, submitted to the COR, via email, that includes a price breakdown by task, travel, and approved ODCs.

F. Schedule of Deliverables

Deliverable	Description
Deliverable 1. **A.**1	Regional Engagement Strategy [within one (1) month of the start of the performance period, then yearly]
Deliverable 1. **A.**2	After Action Reports [within 10 business days of preparedness event]
Deliverable 1. **B.**1	Strategy Implementation Report [quarterly]
Deliverable 1. **B.**2	Regional Preparedness Activity Report [monthly]
Deliverable 1. **B.**3	Monthly FPC Email [5th business day of each month]
Deliverable 1. **B.**4	Bi-Annual Regional Goals and Alignment Report [twice yearly]
Deliverable 1. **B.**5	Bi-Annual Regional Collaboration Report [twice yearly]
Deliverable 1. **B.**6	Annual collaboration report [yearly]
Deliverable 1. **C.**1	Surge Support Team [Up to four times annually]
Deliverable 2. **A.**1	Project Management Plan (PMP) [Delivered at proposal, Reviewed at Kick-Off Briefing 5 business days after award]
Deliverable 2. **A.**2	Project Management Plan (PMP) Updates [Monthly]
Deliverable 2. **B.**1	Project Kickoff Briefing [5 business days after award]
Deliverable 2. **C.**1	Monthly Status Report [5th business day of each month]
Deliverable 2. **C.**2	Monthly IPR Briefing [Monthly]

Deliverable 2. **D.**1	Weekly Status Report [COB Mondays]

For every task, the Contractor shall identify in writing all necessary subtasks (if any) and associated sub- milestone dates. The Contractor's subtask structure shall be detailed in the project management plan (PMP). As indicated in Task 2, Section A, the initial PMP should be submitted with the task order proposal.

After award and during performance of the task order, where a written milestone deliverable is required in draft form, Government will complete its review of the draft deliverable within fifteen (15) calendar days from date of receipt. The Contractor shall have five (5) calendar days to deliver the final deliverable from date of receipt of the Government's comments. There shall be no assumption of approval for any materials, regardless of timeline.

All deliverables shall be delivered to the Contracting Officer Representative (COR) and Government Program Manager (PM).

The PM and COR will attend all meetings and briefings where deliverables or the execution of this task order will be discussed. The Contractor shall include the PM and COR in all communication related to this task order.

All documents must be stored on Government network or other location that has been expressly approved by the COR and Government PM.

The Contractor shall deliver all work products and deliverables throughout the period of performance by the close of business (COB) which shall be 5:00pm EST.

The Contractor shall provide/propose all reporting templates. All reporting templates are subject to ICPD approval and shall be finalized within ten (10) business days of awarding the task order.

G. Travel and Other Direct Costs

While the labor for the tasks described in this PWS shall be provided on a firm fixed price basis, the Government anticipates that other direct costs, including travel, will be required to support these tasks. All such costs shall be approved in advance by the COR and shall not exceed the funding available under the corresponding Contract Line-Item Number (CLIN).

1. Travel

Contractor travel shall be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

The Contractor shall provide the COR with a pre-trip request that is followed up with a post-trip report for any travel that occurred within the previous 30 days as part of the Monthly Status Report for all Government-approved travel.

No local travel shall be reimbursed within a 50-mile radius of the worksite. All travel outside this radius must be approved in advance by the COR.

All contractor personnel may be required to travel on commercial and/or government provided transportation.

Travel, if required, shall primarily occur in the North American continent, including the U.S., Canada, and Mexico. Other travel destinations may include, Hawaii, Alaska, Puerto Rico, and any US Territory.

When authorized as part of the scope of work and as approved by the CO or COR, travel expenses incurred in performance of this PWS shall be reimbursed in accordance with the Federal Travel Regulations (FTR) in effect at the time of travel.

Travel requests must be submitted in sufficient time for the COR to give prior approval, and must identify

the name of the traveler, (ii) destination (s) including itinerary, (iii) purpose of the travel, and (iv) estimated cost breakdown.

To be reimbursed, invoices, including travel expenses, must provide a detailed breakdown of the actual expenditures invoiced. The Contractor shall maintain the original or legible copy of receipts for all travel expenses invoiced. The Government reserves the right to request evidence of any travel expense paid by the Contractor.

This task may require RPL travel up to 15 trips within the Region and 1 trip outside the Region (usually to FEMA HQ) per year. In addition, the Program Manager may make up to 3 trips if needed.

The travel for each period of performance shall have an initial award of up to $80,000.

2. Other Direct Costs (ODCs)

Non-travel Other Direct Costs (ODCs) are anticipated to be required during the performance of this requirement. All Non-travel ODC purchase requests shall be approved by the COR prior to incurring costs. The Contractor shall provide itemized data to support all ODC purchases with appropriate back up information as part of obtaining purchase approval from the Government.

It is anticipated that ODC purchases may be required to print materials under urgent circumstances when GPO process is not feasible due to time constraints. All material must meet FEMA's Office of Disability Integration and Coordination printing requirements.

The non-travel ODCs for each period of performance shall not exceed $50,000, but each period of performance shall have an initial award of up to $10,000.

H. General Contract Requirements and Project Management Techniques

The Contractor shall identify the milestones and task activity that will take place against all project work. The Contractor shall provide a management plan section to provide the resources and cost information as well as the overall management and direction of those resources as part of the plan.

1. Management Structure and Organization

The Contractor shall be capable of ensuring that the following functional requirements, at a minimum, are satisfied throughout the life of the task order:

- Technically proficient and professionally capable contractor personnel maintained throughout the life of the task order. The contractor personnel must work collectively and professionally with any other ICPD contractors. The contractor personnel must maintain knowledge of NPD/ICPD business processes.
- Personnel turnover is minimized, and individuals are motivated to achieve excellent performance. Schedule requirements are met or exceeded to support aggressive deployment schedules.
- Productivity tools, including automated test methods are employed to deliver consistently high-quality services.
- The quality of the products and services provided under this task order is continually monitored throughout the life of the task order.
- Provisions are made to add and/or remove contractor personnel as required by special tasks.

2. Quality Assurance and Continuous Improvement Programs

The Contractor shall be responsible for an effective quality assurance/control program for all deliverables, work products, and services performed under this task order. The Contractor shall institute policies, procedures, and processes that will ensure all products meet task order requirements and will promote "continuous improvement" of the products and processes.

3. Key Personnel

The Contractor shall be required to provide the necessary staff for performance at the ICPD locations and at any off-site locations (Contractor facility) where approved by the COR.

The labor categories listed below reflect anticipated types of personnel that will be necessary for successful task order performance. Required and desired personnel qualifications for these positions are provided. This information is provided for informational purposes only. The Contractor is responsible for providing the necessary staffing with the requisite skill levels needed to accomplish the PWS.

All personnel associated with this task order shall sign a DHS/FEMA Non-Disclosure Agreement. In addition, staff associated with this task shall complete the necessary DHS/FEMA security training.

Before replacing any individual designated as Key by the Government, the Contractor shall notify the Contracting Officer 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 Contracting Officer. The

Contractor shall not replace Key Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as Key for this requirement. Note: The Government may designate additional Contractor personnel as Key at the time of award.

Program Manager

The Program Manager (PM) shall have full authority to act for the Contractor on all contractual matters relating to daily operation of this task order.

A minimum of ten (10) years recent and relevant experience managing a task order of similar size and scope is desired. A bachelor's degree from an accredited college or university is also desired. The Program Manager is identified as a key member of the task order team.

Although not required, a contractor may find it beneficial to include a Deputy PM to support and serve as a backup to the PM.

Regional Preparedness Liaisons

Regional Preparedness Liaisons (RPLs), also known as Emergency Preparedness Program Specialist or Subject Matter Experts, are technical experts called upon to provide assistance on preparedness, communication, or program management. RPLs must be SMEs and shall have demonstrated knowledge of, and prior experience in, all applicable areas to requirements. A bachelor's degree from an accredited college or university is also required.

4. Business Hours

The Contractor shall perform tasks in this performance work statement during normal ICPD daytime business hours, which are 8:30 a.m. – 5:00 p.m. Local Time (for their assigned office). Times may be adjusted if operating in a different time zone or based on field requirements. Provisions may be made for after hour's activities, including weekends and holidays, associated with the normal business of ICPD with COR approval.

5. Place of Performance

Primary place of performance will be co-located with ICPD Federal staff at 400 C Street SW, Washington, DC. Contractors supporting the FEMA regional offices will be physically located within the assigned FEMA regional office.

The FEMA Regional locations are Region 1 (Boston, MA); Region 2 (New York, NY); Region 3 (Philadelphia, PA); Region 4 (Atlanta, GA); Region 5 (Chicago, IL); Region 7 (Kansas City, MO); Region 8 (Denver, CO); Region 9 (Oakland, CA); and Region X (Seattle, WA). Region 6 will not have an RPL.

6. Teleworking

Teleworking by contractor personnel is authorized under this order, but must be approved by regional leadership and the COR. All telework must be conducted in accordance with FEMA policies and guidelines.

7. Performance Period

The period of performance consists of a base period and four option years, as follows. Total task order period of performance: 5 years.

Base Period: April 1, 2023 – March 31, 2024

Option Period 1: April 1, 2024 – March 31, 2025

Option Period 2: April 1, 2025 – March 31, 2026

Option Period 3: April 1, 2026 – March 31, 2027

Option Period 4: April 1, 2027 – March 31, 2028

8. Government Furnished Information, Equipment, and Facilities

Throughout performance of the task order, the vendor shall identify needs for any government furnished equipment (GFE) and submit request for approval and action by COR. The program manager and RPLs must be on site. The Government will provide a FEMA laptop and phone upon successful completion of a background check of the RPLs and Program Manager.

9. Sponsorship

Contractor acknowledges FEMA reserves a royalty free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use, and authorize others to use, for Federal government purposes: (1) the copyright in any work developed under this task order; and (2) any rights of copyright to which the recipient or sub recipient purchases ownership with Federal support.

All materials and/or other publications resulting from this task order shall adhere to DHS/FEMA Logo and Design Standards and FEMA Style Guides. Any use of the DHS logo not addressed by these standards requires preauthorization and approval by FEMA.

Use of DHS Seal: The contractor shall utilize the DHS/FEMA seal and Design Standards when producing training course materials, aids, or other products funded through this award. Any use of the DHS/FEMA seal not addressed by these standards requires preauthorization and approval by DHS.

Use of DHS Seal, Logo, and Flags: All contractors must obtain DHS's approval prior to using the DHS seal(s), logos, crests or reproductions of flags or likenesses of DHS agency officials. Furthermore, use of DHS seals, logos, crests, as approved is limited to the life, intent, and purpose of the immediate task order. Any continued future use of such DHS symbols by the vendor for its' own marketing of materials first developed under this task order, or other purposes beyond the life and purpose of this task order is strictly prohibited, unless permission is first requested by the vendor, and expressly approved in writing by the Contracting Officer.

10. Contractor 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.

11. Security and Privacy

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

Unauthorized Disclosure of Classified or Unclassified Information:

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

Access to the training can be obtained at:

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

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

OPSEC Training:

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

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

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

Insider Threat Training:

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

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

Information Technology Security and Privacy Training (March 2015)

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

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

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

Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent

training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e- mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

Safeguarding of sensitive Information (March 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.

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:

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

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

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

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:

Truncated SSN (such as last 4 digits)
Date of birth (month, day, and year)
Citizenship or immigration status
Ethnic or religious affiliation
Sexual orientation
Criminal History
Medical Information
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.

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:

DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use

Only) Information
DHS Sensitive Systems Policy Directive 4300A
DHS 4300A Sensitive Systems Handbook and Attachments
DHS Security Authorization Process Guide
DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
DHS Information Security Performance Plan (current fiscal year)
DHS Privacy Incident Handling Guidance
Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
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
NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

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

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.

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

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.

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.

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.

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.

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.

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

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

compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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.

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.

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.

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.

Sensitive Information Incident Reporting Requirements. 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.

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:

Data Universal Numbering System (DUNS);
Contract numbers affected unless all contracts by the company are affected;
Facility CAGE code if the location of the event is different than the prime contractor location;
Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
Contracting Officer POC (address, telephone, email);
Contract clearance level;
Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
Government programs, platforms or systems involved;
Location(s) of incident;
Date and time the incident was discovered;
Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
Description of the Government PII and/or SPII contained within the system;

Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system; and
Any additional information relevant to the incident.

Sensitive Information Incident Response Requirements. 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.

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.

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

Inspections,
Investigations,
Forensic reviews, and
Data analyses and processing.

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.

Additional PII and/or SPII Notification Requirements. 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.

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:

A brief description of the incident;
A description of the types of PII and SPII involved;
A statement as to whether the PII or SPII was encrypted or protected by other means;
Steps individuals may take to protect themselves;
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
Information identifying who individuals may contact for additional information.

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:

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

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:

Triple credit bureau monitoring;
Daily customer service;
Alerts provided to the individual for changes and fraud; and
Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

Establish a dedicated call center. Call center services shall include:

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

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

Personal Identity Verification of Contractor Personnel (JAN 2011) (FAR 52.204-9)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall account for all forms of Government-provided identification issued to the Contractor employees in connection with performance under this contract. The

Contractor shall return such identification to the issuing agency at the earliest of any of the following, unless otherwise determined by the Government:

(1) When no longer needed for contract performance.

(2) Upon completion of the Contractor employee's employment.

(3) Upon contract completion or termination.

(c) The Contracting Officer may delay final payment under a contract if the Contractor fails to comply with these requirements.

(d) The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts when the subcontractor's employees are required to have routine physical access to a Federally controlled facility and/or routine access to a Federally controlled information system. It shall be the responsibility of the prime Contractor to return such identification to the issuing agency in accordance with the terms set forth in paragraph (b) of this section, unless otherwise approved in writing by the Contracting Officer.

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

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of1974, Public Law93-579, December 31,1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

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

(a) The Contractor agrees to-

(1) Comply with the Privacy Act of1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)

(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

FAR 52.224-3, Privacy Training

(a) *Definition*. As used in this clause, "personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training, thereafter, is completed by contractor employees who-

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.3 and 39.105).

(c)

(1) "Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover-

(i) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;

(ii) The appropriate handling and safeguarding of personally identifiable information;

(iii) The authorized and official use of a system of records or any other personally identifiable information;

(iv) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise access personally identifiable information;

(v) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and

(vi) The procedures to be followed in the event of a suspected or confirmed breach of a system of records or the unauthorized disclosure, access, handling, or use of personally identifiable information (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).

(2) Completion of an agency-developed or agency-conducted training course shall be deemed to satisfy these elements.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will-

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

Contractor Employee Access (48 CFR 3052.204-71)

(a) Sensitive Information, as used in this clause, means 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, Pub. L. 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.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

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.

Standard OPSEC Training Language

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

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

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

OCSO Required Language for Contracts Including "For Official Use Only" (FOUO) Information

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

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

Contractors and Consultants shall:

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

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

GFE Access to PII

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

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

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

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

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

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

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

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

13. Accessibility

Section 508 Requirements

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

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

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018, and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

Section 508 Requirements for Technology Services

1. 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.

2. 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.

3. When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using

the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The Contractor shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at https://www.dhs.gov/trusted-tester.

4. When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at https://www.dhs.gov/compliance-test-processes.
5. When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester
6. Contractor personnel shall possess the knowledge, skills, and abilities necessary to address the accessibility requirements in this work statement.

Section 508 Deliverables

1. **Section 508 Test Plans**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.
2. **Section 508 Test Results**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.
3. **Section 508 Accessibility Conformance Reports**: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found

at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

4. **Other Section 508 Documentation**: The following documentation shall be provided upon request for ICT items offered through this contract:
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Documentation of core functions that cannot be accessed by persons with disabilities.
    - Documentation of remediation plans to address non-conformance to the Section 508 standards

Attachment 1: Quality Assurance Surveillance Plan

1. CONTRACT SERVICES TITLE

Regional Support for Individuals and Community Preparedness and Outreach

2. WORK REQUIREMENTS

In accordance with the PWS Tasks, and specifically the Performance Requirement Summary (PRS below), the requirements to be monitored under this contract apply to PWS Section E Tasks.

3. PRIMARY METHOD OF SURVEILLANCE

100 % inspection of work deliverables as contained in the PWS as addressed in the PRS. The PRS is organized as follows:

- Column 1 - Performance Requirement (PR) lists the PR that the government will monitor. The absence of any contract requirement from the QASP/PRS shall not detract from its enforceability nor limit the rights or remedies of the Government under any other provisions of the task order.
- Column 2 – Standard. Defines each specific area to be monitored.
- Column 3 – Performance Requirement. Defines standard that must be met.
- Column 4 – Surveillance Methods – Indicates the method(s) of surveillance the Government will use to evaluate the contractor's performance for the listed tasks
- Column 5 – Evaluation and Incentives. Describes both positive and negative incentives.

4. SCOPE OF PERFORMANCE:

Deliverable	Description	Assessor(s)
Deliverable 1. **A.**1	Regional Engagement Strategy [within one (1) month of the start of the performance period, then yearly]	COR/PM
Deliverable 1. **A.**2	After Action Reports [within 10 business days of preparedness event]	COR/PM
Deliverable 1. **B.**1	Strategy Implementation Report [quarterly]	COR/PM
Deliverable 1. **B.**2	Regional Preparedness Activity Report [5th business day of each month]	COR/PM
Deliverable 1. **B.**3	Monthly FPC Email [5th business day of each month]	COR/PM
Deliverable 1. B.4	Bi-Annual Regional Goals and Alignment Report [twice yearly]	COR/PM
Deliverable 1. **B.**5	Bi-Annual Regional Collaboration Report [twice yearly]	COR/PM
Deliverable 1. **B.**6	Annual Collaboration Report [yearly]	COR/PM
Deliverable 1. **C.**1	Surge Support Report [NTE four times annually]	COR/PM
Deliverable 2. **A.**1	Project Management Plan (PMP) [Delivered at proposal, Reviewed at Kick-Off Briefing 5 business days after award]	COR/PM

Deliverable 2. **A.**2	Project Management Plan (PMP) Updates [Monthly]	COR/PM
Deliverable 2. **B.**1	Project Kickoff Briefing [5 business days after award]	COR/PM
Deliverable 2. **C.**1	Monthly Status Report [NLT 5th business day of each month]	COR/PM
Deliverable 2. **C.**2	Monthly IPR Briefing [NLT 10th business day of each month]	COR/PM
Deliverable 2. **D.**1	Weekly Status Report [Weekly - COB Monday]	COR/PM
Quarterly Survey*	Quarterly General Assessment of RPL Support	Federal Technical Monitor/COR/PM

*Federal Technical Monitors for each RPL will complete a quarterly survey to assess overall RPL performance.

5. EVALUATION METHODS:

- Direct Observation – Periodic or 100% surveillance by federal staff at FEMA HQ and/or at the regional offices.
- User Survey – Quarterly surveys administered to regional federal staff.
- Validated Customer Complaints – Reviewing and evaluating complaints from regional offices through user surveys or otherwise.
- 100% Inspection – The Government will review and either accept or reject all deliverables.

6. PERFORMANCE REQUIREMENTS SUMMARY

Performance Requirement	Standard	Acceptable Quality Level (AQL)	Surveillance Methods	Incentives
Administration & Management	Must perform in accordance with the performance standards as prescribed in the PWS	100% compliance to performance objectives	Direct Observation	The Government will document the failure to meet the performance standard and may include in contract evaluations. The Government will document and share successful performance in government past performance systems.

Deliverables & Service - Quality	Achieve 100 % satisfactory rating Perform 100% in accordance with the performance standards as prescribed in the PWS Conform 100% to the Government Printing Office (GPO) Manual as well as DHS and FEMA writing style and standards Must be 100% error free (e.g., content, spelling, grammar, formatting, punctuation, etc.)	95% compliance to performance objectives	Direct Observation User Survey Validated Customer Feedback 100% Inspection	Government will document the failure to meet the performance standard and may include in contract evaluations. The Government will document and share successful performance in government past performance systems.
Deliverables and Service - Schedule	Must be submitted by the agreed upon or established due dates	100% compliance to performance objectives	Direct Observation User Survey Validated Customer Feedback 100% Inspection	Government will document the failure to meet the performance standard and may include in contract evaluations. The Government will document and share successful performance in government past performance systems.