Attachment 1

Individual and Community Preparedness Division (ICPD) Headquarters Programmatic Support Services

Performance Work Statement

09/03/2024

A. Table of Contents

B. 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 a requirement for program support; research, analysis, and evaluation; and creative content and outreach to support the mission to increase individual and community preparedness, bolster resilience and reduce risk.

ICPD's goal is to reduce suffering caused by disasters with a focus on those living in and supporting the needs of underserved communities. Success is a culture where preparedness is part of everyday life wherein individuals and communities know their relevant hazards, have taken actions to prepare for and reduce risks from those hazards and are thus less dependent on post disaster assistance from all levels of government. This contract will support these efforts.

C. Background

Organizationally, ICPD is in the Risk Management Directorate of the Resilience component within FEMA. ICPD works to strengthen our Nation's resilience by preparing individuals, organizations, and communities for all hazards emergencies. ICPD conducts research to enhance understanding of effective preparedness actions and ways to motivate the public to take those actions. In addition, ICPD develops and shares preparedness and risk reduction resources and coordinates comprehensive disaster preparedness and risk reduction initiatives to help individuals and communities prepare for, protect against, and respond to disasters. ICPD achieves this mission through close coordination with the FEMA Regions; federal, state, local, tribal, and territorial agencies; and nongovernmental partners from all sectors.

ICPD is FEMA's primary developer of programs, tools, training, and gaming for individuals, organizations, and communities. Within FEMA and in partnership with other Federal agencies, ICPD encourages the incorporation of research-based, inclusive emergency management principles all to improve the state of individual and community preparedness. The Division's

programs and initiatives fall into five portfolio areas including Community Responder, Capacity Building, Personal Resilience, Preparedness Actions, and Youth Preparedness. In addition, the Division conducts outreach through various means and has a robust preparedness research capability.

D. Scope

ICPD creates programming that builds the capabilities of individuals and families prepare for the hazards they may face. ICPD programs empower U.S. residents and community-based organizations to become active participants in risk reduction activities. ICPD's research informs actions taken by individuals and communities across the nation to stay safe before, during, and after a disaster. This contractor shall provide the government with support in areas including, but not limited to:

- Contract Administration and Management
- Portfolio Program Support
    - Capacity Building (Organizations Preparing for Emergency Needs, Are You Ready, Building a Roadmap to Resilience, Ready Campus, Ready Business, etc.)
    - Community Responder (Until Help Arrives, training and doctrine development for Community Emergency Response Teams, etc.)
    - Personal Resilience
    - Preparedness Actions (Protective Actions, Individual and Community Preparedness Learning Agenda, Hazard Information Sheets, etc.)
    - Youth Preparedness (Youth Preparedness Council, Student Tools for Emergency Planning, Prepare with Pedro, Child Safeguarding, Ready, Summit event planning, etc.)
- General Administrative Support
- Outreach Support
    - Constituent Communications
    - Conference and Partnership Management
    - Resource Management
    - Translations
- Research, Analysis, and Evaluation
    - National Household Survey
    - Program Analysis and Evaluation
    - Surveys
    - Focus Groups
    - Cognitive Testing
    - Focused Interviews
- Materials, Printing, and Travel

E. Performance Summary Requirement

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. In addition, written documents shall use plain language and shall be concise and clearly written. The Contractor shall ensure the accuracy, functionality, completeness, professional quality, and overall compliance with government guidelines/requirements, including the latest FEMA Branding and Writing Style guidance, of the deliverables.

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

F. Tasks and Requirements

1. Task 1: Administration and Management

The Contractor shall provide management and oversight of all contract activities and deliverables. All support for FFP portions of this task will be accomplished using the LCATs and LOE prescribed below. Contractors may use additional LCATs if deemed necessary. In addition to a Program Manager, Tasks 2-4 shall each have a General and Operations Manager hereto known as Task Lead.

A. Project Management Plan (FFP)

The Contractor shall provide a detailed draft Project Management Plan (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 shall include specific sections, identified below, which present the Contractor's plan for completing the work describing the technical approach, management plan, organizational structure and resources, and management controls that will meet the objectives of this PWS. The Contractor's plan 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 final PMP (1.A.1) shall be submitted 10 business days after the kick-off. The Contractor shall keep the PMP up to date throughout the period of performance; specifically, the Contractor shall provide monthly recommended updates in the form of tracked changes in Microsoft Word. Further, the Government may, at any time, request additional updates that shall be completed by the Contractor and delivered to the Government no more than 10 business days after the request. These updates may include the addition of activities not included in the initial plan. An Annual PMP Update (1.A.2) shall be submitted within ten (10) business days of the start of each Option Year.

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 contract. The goal of the plan is to ensure the contract support staff is properly aligned to the strategic goals, mission, and objectives of FEMA. The staffing plan shall also include the Contractor's organizational structure in support of the contract. 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, cost, or timeliness of services. Only trained staff shall be permitted to work in support of this contract (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 Contractor's roles and responsibilities of 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 Task 1: Part D.
- Quality Control Plan (QCP): The QCP shall provide specifics regarding how the Contractor defines, implements, and assures quality and compliance to the QASP during the contract 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 the tasks below as well as the Key Personnel section of this document. The Contractor shall outline a plan for how staff who support 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 to ensure 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. *All tasks must be fully*

transitioned from the incumbent no later than August 20, 2024, one week prior to the end of the incumbent's period of performance.

- 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 60 days prior to the end of the contract. 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 contract close-out meetings leading up to the end of the contract. 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.
- Deliverable Submission Schedule: The Contractor shall provide a submission schedule for all Task 1 deliverables in the Base period of performance.
- Subcontract Management Plan: The Contractor shall provide a subcontract management plan that details the subcontract management approach. In addition, this plan should list all proposed subcontracts.

Deliverable 1.A.1 – Project Management Plan (PMP) [Delivered NLT ten (10) business days after Kick Off Briefing]

Deliverable 1.A.2 – Annual Project Management Plan (PMP) Update [Delivered NLT ten (10) business days after the start of each Option Year].

B. Contract Kick-Off Briefing (FFP)

The Contractor shall host a project Kick-Off Briefing (1.B.1) with Government project team. The Kick-Off Briefing shall be held within 5 business days after contract award or as agreed upon between the Government and Contractor. The kick-off meeting shall be in-person at FEMA headquarters in Washington, DC. At the Kick-Off Briefing, the Contractor shall, at a minimum, brief the details of the Project Management Plan (PMP).

C. Monthly Interim Progress Review and Report (FFP)

The Monthly Interim Progress Review (IPR) is typically a meeting that 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, budget, and risk. The

Contractor shall provide an IPR Briefing Deck (1.C.1) to guide the meeting. The IPR Briefing Deck may draw heavily from the Monthly Status Report.

The Contractor shall provide a Monthly Status Report (MSR) (1.C.2) to the Government, electronically, no later than the 5th business day of each month. This MSR shall cover all contract related activity for the previous month. For example, the MSR delivered on the 5th of November shall detail all activity occurring in the month of October.

The MSR shall present the work accomplished during the previous month. This report shall also identify any problems that arose and a statement explaining how the problem was resolved. Further, the 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:

- Organization 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 toward completion of the POP;
- Identification of project risks;
- Summary of the tasks and work products completed; and
- Status of deliverables.

Deliverable 1. C.1 Monthly IPR Briefing Deck [NLT 10th business day of each month]

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

D. Weekly Reporting (FFP)

The Weekly Status Report (WSR) (1.D.1) shall highlight risks and issues as well as any outstanding items. Risks and issues shall be reported weekly as critical, high, medium, or low. A description shall be included of the risk/issue, the owner, progress made, and management or risk mitigation 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 contract. The WSR shall be delivered via email to both the COR and PM on the first business day of each week. Feedback from Government staff must be reflected in the subsequent submission.

Deliverable 1. D.1 Weekly Status Report [2nd business day of each week]

In addition to the WSR, the contractor shall provide a weekly budget update for all Time and Material tasks (1.D.2). The update shall be in the form of a tracker which at a minimum, shows the following information:

- Name of task;
- Approved task budget;

- Percentage of the budget used;
- Burn rate;
- Risks; and
- Comments

Deliverable 1. D.2 Weekly Budget Report for T&M Tasks [2nd business day of each week]

E. Administration (FFP)

The Contractor shall complete standard administrative tasks (e.g., background investigation forms, staff roster, mandatory training, etc.). Project staff members must not start work on projects until the COR has received a fitness form and a signed non-disclosure agreement.

Invoices must be submitted monthly using SF 1034 and SF 1035. In addition, all invoices must include an Excel spreadsheet that includes a price breakdown for each T&M task as well as Other Direct Costs (ODC). This will help government program managers and CORs track and validate the work performed and the ODCs.

2. Task 2: Program and Administrative Support

The ICPD has five portfolio areas including Capacity Building, Community Responder, Personal Resilience, Preparedness Actions, and Youth Preparedness. Each portfolio has subordinate programs. ICPD leadership will prioritize and select three programs to update during each period of performance (PoP). The Contractor shall assist in making these program updates to revise products and enhance their effectiveness. In addition, under FFP the Contractor shall provide support for program operation and development of material and strategies to help engage stakeholders. All support for FFP portions of this task will be accomplished using the LCATs and LOE prescribed below. The Task Lead (listed under Task 1: Admin and Management) will manage all FFP and T&M activities under Task 2. The Contractor must provide the LCATs and LOE prescribed below.

In addition to the FFP support, the Contractor shall provide T&M activities as needed to include administrative support, surge support, and program development. All T&M tasks will be supported using the aforementioned and other LCATs as necessary.

Note: Research, analysis and evaluation activities may be requested to support any of ICPD's portfolios, but this support will fall under Task 4 as T&M.

Deliverable 2: Program Updates *[Three (3) Annually]*

The following sections provide portfolio information and identify some of the potential activities that could constitute program support under FFP. Government PMs will coordinate with their leadership and the Task 2 Lead to develop portfolio task plans. These task plans will prescribe work activities and balance the anticipated level of effort. In addition, some sections will describe the support needed, upon request, for T&M activities.

A. Capacity Building Portfolio (FFP)

Community-based organizations (CBO's), faith-based organizations (FBO's), small businesses, and other non-profits provide critical services to communities before, during, and after an emergency. ICPD develops continuity training and risk reduction tools for these organizations to become resilient ahead of disasters to ensure they can continue serving their communities throughout their recovery.

Current programs include, but are not limited to: Building a Roadmap to Resilience: A Whole Community Training, OPEN Training, and Are You Ready? A Guide to Citizen Preparedness

1. **Building a Roadmap to Resilience: A Whole Community Training (E426)**

E426 is a classroom-based training typically offered at the National Emergency Training Center in Emmitsburg, MD. This course aims to provide students with the knowledge and tools to engage their whole communities and help community groups move beyond basic awareness. By the end of the training, students will have customized roadmaps for establishing a community resilience coalition and a plan to encourage community leaders to make resiliency gains within the unique circumstances of their jurisdictions.

2. **Organizations Preparing for Emergency Needs (OPEN) Training**

OPEN includes both a web-based, self-guided training, and a downloadable instructor kit that will guide participants on how to identify risks, locate resources, and take preparedness actions. When Community-Based Organizations, such as food pantries, daycares, and non-profits, are unable to sustain operations during an emergency incident, individuals who rely on them are exponentially impacted. Because of their importance in keeping the community going, OPEN is designed to empower these organizations to better prepare for incidents.

3. **Are You Ready? A Guide to Citizen Preparedness**

In September 2020, FEMA released the Are You Ready Guide. The guide emphasizes the importance of preparing for disasters, highlights the need to know your risks and the best actions to protect yourself and others, encourages plan creation, recommends specific actions, and provides general guidance to help in the recovery process. This guide is available online.

B. Community Responder Portfolio (FFP)

ICPD educates volunteers about disaster preparedness for the hazards that impact their area, and trains them in basic disaster response skills through in-person and virtual trainings.

Community Responder programs provide valuable resources for individuals and communities. Program promotion proves is necessary to raise awareness and encourage communities to leverage these programs to enhance their overall preparedness postures.

The Contractor shall develop Community Responder Promotional Packages when requested to support program or product rollouts and improvements.

Current programs include Community Emergency Response Team (CERT), and You Are the Help Until Help Arrives (Until Help Arrives) (UHA).

1. **Community Emergency Response Teams (CERT)**

CERT educates volunteers about disaster preparedness for hazards that may impact their area and trains them in basic disaster response skills such as fire safety, light search and rescue, team organization, and disaster medical operations. CERT offers a consistent, nationwide approach to volunteer training and organization that professional responders can rely on during disaster situations, which allows them to focus on more complex tasks.

2. **You are the Help Until Help Arrives (UHA)**

UHA is a program designed to educate and empower the public to take action in emergency situations and provide lifesaving care before professional help arrives. Through online instruction and in-person trainings, participants are trained to take action and, through simple steps, potentially save a life. Materials developed for this educational campaign include a 2.5-hour instructor-led course, a 30-minute web-based training module, and an interactive video.

C. Personal Resilience Portfolio (FFP)

Personal Resilience is an individual's ability to overcome a challenge. By recognizing everyone is capable of being resilient in different ways, Personal Resilience aims to remove barriers to preparedness. Programming for the Personal Resilience portfolio includes work that will support four pathways of resilience: Emotional, Financial, Physical, and Social.

The Contractor will support the government in strengthening the national Personal Resilience posture. Examples of work under this portfolio may include, but are not limited to:

- New programmatic work: Design, implement, and maintain new programs in the four pathways of Personal Resilience. These programs should be novel and targeted for individuals and communities. (This would fall under New Programs T&M.)
- Existing programmatic work: Update, enhance, or maintain existing programs in the four pathways of Personal Resilience These programs can update current ICPD or FEMA preparedness programs, or programming from other federal agencies or non-profit organizations ICPD has an MOU with. The programs should be targeted for individuals and communities.
- Implementation: Implement the above programmatic work in targeted communities.
- Technical Assistance: Provide technical assistance to the targeted communities on the new or existing programmatic work.
- Communication Strategy: Create engagement materials that communicate the successes or current status of the Personal Resilience for internal and external stakeholders. Promotion also entails communication materials and potential engagement opportunities.

The government may request the Contractor to conduct evaluation of Personal Resilience program data. Additionally, the government may request support to conduct Focus Groups to test the impact of personal resilience. Such analysis will be priced and approved under the Research, Analysis and Evaluation task under T&M.

The descriptions below provide examples of Personal Resilience programs.

1. **Emergency Financial First Aid Kit (EFFAK)**

Developed in coordination with Operation Hope, the EFFAK is a product that helps individuals collect, organize, and store critical financial, medical, and household information. The EFFAK includes a checklist of important documents and forms and offers peace of mind for having this information readily available.

2. **Your Disaster Checklist**

Developed in coordination with the Consumer Financial Protection Bureau (CFPB), the Your Disaster Checklist tool helps users collect, copy, and store financial and other information that will help users avoid problems and recover faster after a disaster.

D. Preparedness Actions Portfolio (FFP)

1. **Protective Actions**

Protective Actions are research-based actions and advice that anyone can take to prepare for, keep safe during, and recover from a disaster. Over 15 hazards have validated and published protective actions.

The Contractor shall provide support for research, graphics, and research site updates and enhancements. In addition, the Contractor shall propose additions and updates to content for Protective Actions site based on the outcomes of protective actions research activities. In addition, the Contractor will be responsible for coordinating and executing content upload to the site.

Research

ICPD's Protective Action Research informs key messages for individual- and community-focused FEMA products and interagency coordination. To date, this effort has informed content on FEMA's Community pages, ready.gov, hazard information sheets, and preparedness products such as Are You Ready, among others. The Contractor may conduct research (through literature review, evaluation, and receiving and the integration of partner feedback) to identify the best protective actions for new hazards or revalidate existing protective actions.

Graphics

The Protective Actions graphics efforts support the Division's efforts to communicate Protective Actions research to the whole community. Specifically, visual products to assist with and bolster user learning retention. The Contractor shall create graphics for the new or updated protective actions. Graphics may include, but are certainly not limited to, icons, individual graphics, and hazard information sheets.

Research Site

In 2020, ICPD began the process of uploading the content from individual static (Word document) reports onto the FEMA Community Pages' Protective Actions Research site https://community.fema.gov/ProtectiveActions/s/. The reports published in this online tool are 508 compliant to ensure accessibility. The research, messaging, and recommendations on the site provide decision-making guidance to individuals and households, messaging guidance for practitioners, and research recommendations for researchers in the disaster preparedness space. The goal of the site is to inform messaging, provide decision-making guidance, and encourage researchers to collaborate with FEMA to enhance the research so that the Agency can continue to provide the best guidance to the public.

2. Hazard Information Sheets

Validated protective actions enable ICPD to create and update hazard information sheets. FEMA's Hazard Information Sheets (usually about two pages each) provide the public with clear, concise, plain language messaging and include important information about a hazard, its impacts, and ways to prepare for, keep safe during, and recover from a disaster. Individuals and community organizations can use these hazard information sheets to promote preparedness for potential hazards in local areas.

The Contractor shall support the government in developing and updating hazard information sheets.

3. Individual and Community Preparedness Learning Agenda

In 2021, ICPD engaged with over 200 stakeholders from over 140 organizations across the continental United States, Hawaii, Alaska, and Puerto Rico as part of a Whole Community approach to develop the Individual and Community Preparedness Learning Agenda. With the understanding that preparedness is a shared responsibility and should involve the whole community (individuals and families, including those with access and functional needs; businesses; faith-based and community organizations; nonprofit groups; schools and academia; media outlets; all levels of government, including state, local, tribal, territorial, and federal partners) the Learning Agenda is a tool to help strategically organize important questions, drive research, and generate evidence.

ICPD will continue the outreach implementation for the Individual and Community Preparedness Learning Agenda by first engaging with the Regions through the Regional Preparedness Liaisons and Community Preparedness Officers. ICPD will engage with these stakeholders to better understand their interest in ICPD's ongoing research efforts and to better understand what data they have that they may be able to contribute toward the generation of data for questions. ICPD will also encourage the regions to engage their local partners to generate data.

The Contractor may support efforts to further promote the learning agenda and engage and encourage stakeholders to collect and share data that may help answer learning agenda questions. Specifically, the Contractor may assist in develop/update a promotional package to include strategy and promotional products (e.g., webinars, listening sessions, learning agenda website updates, draft outreach communications, etc.)

In addition, the government may request the Contractor to conduct analysis of Learning Agenda data. Such analysis will be priced and approved under the Research, Analysis and Evaluation task under T&M.

E. Youth Preparedness Portfolio (FFP)

Youth preparedness programs empower children with resilience skills necessary to stay safe during disasters while harnessing youth as change agents within their communities to increase resilience across the country.

Current programs include, but are not limited to: Youth Preparedness Council, Integrating the Needs of Children (INC) Workshop, Prepare with Pedro, STEP, and Ready 2 Help. The level of effort for Youth Preparedness Council and the Youth Preparedness Summit may be supplemented with Surge Support under T&M.

1. Youth Preparedness Council

The FEMA Youth Preparedness Council was formed in 2012 to bring together youth leaders in grades 8-11 from across the country who are interested and engaged in advocating for preparedness. The Council is made up of 15 members who are selected based on their dedication to public service, their efforts in making a difference in their communities, and their potential to expand their impact as national advocates for preparedness.

During their one-year term, members complete preparedness projects and share their opinions and experiences regarding youth disaster preparedness with FEMA leadership and other preparedness organizations. Examples of members' projects have included starting preparedness programs in schools and communities, helping to establish state youth preparedness councils, developing a mobile application for first responders, and hosting disaster preparedness exercises and events.

The Contractor shall provide general support for the YPC Council. Such support may include but is not limited to providing administration support for the Council application, selection, and onboarding processes, including the development and execution of a tracking system for applications and members; program support for the Council and member preparedness projects, including the design of educational materials; collecting, analyzing and reporting program metrics; and developing After-Action Reports.

2. Youth Preparedness Summit

ICPD hosts a biannual YPC Summit in the National Capital Region, bringing together graduating and incoming YPC members to participate in team building activities, learn about emergency management and project planning, attend media training, and hear from Emergency Management leaders from across the country.

The Contractor shall provide logistics and planning support for hosting the bi-annual event. In addition, the Contractor shall also provide an after-action report that covers the event, application process, review process, and internal reports (such as weekly emailed reports tracking the number of submissions, progress of application reviews or after-action reports from the annual

YPC Summit). Although this includes preparing a FEMA conference approval package and arranging the logistics, the contractor is not required to provide the venue; however, that may prove a viable option.

3. Youth Programs (Pedro, STEP, Ready 2 Help, INC, Child Safeguarding, etc.)

ICPD has a number of Youth Programs aimed to develop youth preparedness or protect youth. The contractors shall support the government in strengthening the youth programs. Examples of work may include, but are not limited to, expanding, or revising/updating existing programs, providing support for updated program implementation, and executing projects. In addition, the government may request the Contractor to conduct analysis of youth program data. Such analysis will be priced and approved under the Research, Analysis and Evaluation task under T&M. In addition, the Contractor will support the development and implementation of engagement materials for ICPD to communicate and engage with partners and the public.

The following are some examples of Youth Programs some of which may require ongoing support.

Prepare with Pedro

This award-winning program was created by the American Red Cross with FEMA leading efforts grow the brand and expand product offerings. This suite of youth preparedness products follows Pedro the penguin as he learns about how to be prepared for and take action during various hazards and emergencies to help stay safe. This program is traditionally taught in classrooms and presented through a storybook, accompanied by workshops and games, to students in kindergarten to second grade (ages 4-8).

STEP

Student Tools for Emergency Planning (STEP) is an emergency preparedness curriculum for students in the fourth grade and older that can be taught in the classroom or other settings, such as after-school programs or scouts. Students learn about disasters, emergencies, and hazards; how to create a disaster supply kit; and family emergency communication planning.

Ready 2 Help

Ready 2 Help is a fun card game that teaches children ages 8–12 developmentally appropriate skills to respond to emergency situations in five simple steps: Stay Safe, Stay Calm, Get Help, Give Info, and Give Care. This game helps to teach kids how to stay safe and make a difference until help arrives. With the Ready 2 Help card game, players can respond to examples of emergencies by working with their friends and using skills that will help them in a real emergency.

INC

The Community Preparedness: Integrating the Needs of Children (INC) workshop is a way to encourages collaboration between local governments, emergency management professionals, and a diverse array of community-based organizations that serve children by bringing them to the table and deliberately plan for children during disaster situations. This community-based workshop promotes community planning, coordination, and integration of children's needs during emergencies. Using established planning methodologies, the workshop walks participants

through identifying the organizations, requirements, and resources needed in their preparedness programs to ensure that children are kept safe and healthy during disasters.

Child Safeguarding

Child Safeguarding is the policies, processes, and practices that make organizations and their people safe for children. It is the responsibility of ICPD as a provider of youth programs to consider the minors that are recipients of these efforts and ensure they are being protected and their well-being is taken into consideration throughout the programmatic cycle.

F. New Programs (T&M)

Based on Division needs and Agency priorities, the division may add to the existing suite of preparedness programs. As such, the Contractor shall provide developmental support for new programs as needed. Programs may be in any of the portfolio areas and may also include curriculum development and preparedness animations. The government PM shall develop a task plan for new program development and the government and Contractor shall develop and agree upon a budget.

Deliverable 2. F **New Program *[as needed]***

G. General Administrative Support (T&M)

The Contractor shall provide the following general administrative, operational, and secretarial support tasks to government executive managers. This level of effort will typically not exceed 20 hours/week. The Contractor shall conduct any or all the following at the government's request:

- Schedule appointments/meetings;
- Manage and monitor calendars and daily itineraries;
- Relay Executive manager availability and whereabouts;
- Manage Outlook in-boxes and calendars;
- Develop short/long range operational schedules;
- Coordinate travel arrangements; travel schedules to include status of orders and itineraries, transportation, and accommodation arrangements;
- Arrange meetings/conferences and prepare appropriate background material;
- Generate and manage correspondence to include electronic mail and forward correspondence to appropriate personnel;
- Utilize computer software, primarily Microsoft Word, Excel, Power Point and Outlook to type, prepare, store, transfer, and print documents including letters, memoranda, forms, reports, charts, graphs, and presentations from handwritten or electronic drafts or from supplied samples and provided data;
- Review all documents and correspondence for format, grammar, and punctuation in accordance with the FEMA Writing Style Guide and the U.S. Government Printing Office Style Manual;
- Prepare and send documents via electronic methods, U.S. Mail, or use of overnight delivery services (or a combination of more than one); and
- Provide notes, as needed, for special events or meetings.

H. Surge Support (T&M)

For a number of possible reasons, the government may need to surge support to accomplish organizational goals and objectives. For example, disaster declarations may result in federal employee deployments to support disaster operations and require additional support from contract staff to maintain continuity. The contractor shall provide surge support, as needed, in relation to any other sections of this PWS.

3. Task 3: Outreach Support

A. Constituent Communications (T&M)

1. Newsletters

The Contractor will plan, develop, and deliver the ICPD newsletter (3.B.1). The newsletter will be distributed quarterly. In addition to the newsletter, supplemental "news blasts" may prove necessary to highlight special events, webinars, or ICPD program and product updates.

The Newsletter will support the Federal Emergency Management Agency's Individual and Community Preparedness Division's (ICPD) goal of achieving a culture of preparedness for the U.S. population by offering preparedness tips, resources, and the latest news on preparedness initiatives, ICPD programs, and preparedness events across the Nation. The priorities of the Newsletter are to feed into FEMA's wider mission to help the Nation before, during, and after disasters as well as ICPD's mission to connect individuals, organizations, and communities with research and tools that help to build and sustain capabilities and prepare for any disaster or emergency. These are to:

- Build awareness of hazards and preparedness strategies, ICPD programs and publications, and partner resources;
- Help readers find and share promising practices, relevant research, accessible learning opportunities, and engaging stories of promising practices and successful initiatives;
- Encourage readers to take preparedness actions and support others in their community to do the same;
- Support partner engagement by providing a platform to share content; and
- Influence preparedness conversations and highlight FEMA priorities.

Deliverable 3.A.1.1 Newsletter [quarterly]

Deliverable 3.A.1.2 News Blasts [as assigned]

2. Data Digest

The Contractor shall plan, develop, and deliver up to six (6) Data Digests annually which may include themes (e.g., based on hazard or demographic data), address National Preparedness Month (NPM), or summarize the National Household Survey Data (3.B.2).

The Data Digest is a tool for promoting awareness of ICPD's research and for encouraging stakeholders and partners to discover and apply key findings that are relevant to their communities and customers to their own preparedness messaging and programs. The Data Digest

is distributed to hazard and preparedness Subject Matter Experts, researchers, and communications experts at other Federal Agencies and academic institutions. It is also published to FEMA's Community Pages. Ultimately, the Data Digest provides ICPD research-based information and graphics for local emergency managers, community-based organizations, and educators, who can integrate the key findings into their work with local communities.

Deliverable 3.A.2 Data Digest [Up to 6 annually]

3. Webinars

The Contractor shall provide technical support to schedule, develop, and host up to 12 webinars annually. Webinars typically last between 30 and 60 minutes. Content development will fall under the programs. For example, content for a Personal Resilience webinar would be considered FFP under the Personal Resilience work whereas a webinar for the National Household Survey (NHS) would be considered T&M under the NHS work.

The Government has historically used Adobe Connect to host the webinars but may elect to use other platforms as needed. In addition to webinar support, the Contractor will secure the annual continuation of current licensing. Requirements defined in ODCs. The Contractor will also ensure that webinars are inclusive of individuals with hearing, visual or other disabilities.

Deliverable 3.A.3 Webinars [as assigned]

B. Resource Management (T&M)

Warehouse Maintenance and Document Publication Support

The FEMA Warehouse maintains an inventory of preparedness products, with highly demanded products translated into 5 languages other than English, available free for any member of the public to order. These products support and accomplish FEMA's goal of building a culture of preparedness across the whole community. ICPD has the responsibility to ensure the Warehouse has products to distribute. ICPD has established a standard operation procedure (SOP) for monitoring and managing Warehouse inventories.

The contractor will review and update the Warehouse SOP on an annual basis (3.C.1) to ensure that it includes up-to-date information about ICPD products, POCs, and processes. The Contractor will submit the recommended updates to ICPD for review and approval.

The Contractor shall maintain and/or enhance existing inventory tracking tools.

The Contractor will prepare a biweekly (twice a month) stock status report (3.C.2) per the instructions provided in the Warehouse SOP.

The Contractor will be available to provide support in the preparation of ICPD product publications printing packages to Government Printing Office (GPO) specifications, ensuring the correct formats, design attributes, and other details for documents are provided to accurately produce physical printed materials by the FEMA in-house print shop, GPO or GPO sourced vendors.

The Contractor will provide a monthly budget report (3.C.3) using the procedure established in the Warehouse SOP. The Contractor will flag any low balances or cautions if the number of

products ordered exceeds the amount of funding in the account. The report shall include recommendations for moving forward. The Contractor will share the budget report with Government Program managers.

Deliverable 3.B.1 **Warehouse SOP Updates [annually]**

Deliverable 3.B.2 **Stock Status Report [bi-weekly]**

Deliverable 3.B.3 **Budget Report [monthly]**

C. Translations (T&M)

ICPD is committed to ensuring that people with limited English proficiency (LEP) have access to disaster preparedness materials. Accordingly, ICPD aims to provide written, electronic, and multi-media material in multiple languages.

The Contractor will assist ICPD in providing translation services including, but not limited to, foreign language translation, foreign language interpretation, transcription translation/captioning services, voiceovers in the selected foreign language, website localization, 508 compliance, and desktop publishing. As applicable, translation work may require coordination with FEMA's External Affairs; however, ICPD will be responsible for that coordination.

Language proficiency testing in the source language(s) and English is required for all levels of linguists in the four basic communications skills (listening, reading, writing, and speaking). Evidence of language proficiency testing with acceptable results from an organization listed herein (below) is required to be submitted to the COR for all linguists prior to assignment to this contract. Testing shall have occurred no more than five years in the past. In-house testing by companies that provide linguistics services will not be accepted. FEMA will not reimburse fees charged for language proficiency testing and/or costs associated with state certification, e.g., training and travel.

The minimum acceptable language proficiency standards are as follows:

- By U.S. Government Agencies: Members of the Interagency Language Roundtable (Department of State/Foreign Service Institute; Department of Defense/Defense Language Institute; Department of Justice/Federal Bureau of Investigation; Peace Corps; United Nations) provide written and oral proficiency tests in a variety of languages. A proficiency rating of 3 or above in speaking, listening, reading, writing, and congruity judgment in the foreign language and a proficiency rating of 3 or above in speaking, listening, reading, writing, and congruity judgment in English is required.
- By the Federal Court Interpreters Certification Program: Certification as a Court Interpreter by the Administrative Office of the U.S. Courts is acceptable. This certification is provided only for Spanish to/from English, Navajo to/from English, and Haitian Creole to/from English.
- By the State Courts: Certification or inclusion on the Registry of Tested Interpreters by any of the members of the Consortium for State Court Interpreter Certification is acceptable proof of language proficiency: A current list of member States is available at

www.ncsconline.org/D_research/index.html; click on "Court Interpretation"; click on "Consortium for Language Access in the Courts"; and click on "Which states belong to the consortium?" The languages that are certified or tested vary depending on each State's requirements.

  - NOTE: Although successful test results and certification by the Federal and State court systems are acceptable as proof of language proficiency, certified or qualified court interpreters are not required on this contract unless a certified or qualified court interpreter(s) is the subject of a Task Order. Any certified/qualified court interpreters that are assigned to other linguistic duties on this contract will be paid at the rate for the labor category to which assigned; e.g., although a Shift Supervisor for the Spanish language possesses certification by the Administrative Office for the U.S. Courts to perform as a court interpreter, he/she will be paid at that Shift Supervisor rate when performing those duties on this contract.

- By Private Language Testing Institutions: A = Advanced, S = Superior, or H = High skill levels in speaking, listening, reading, and writing in the source language and speaking, listening, reading, and writing in English are acceptable. Low, novice, and intermediate skill levels of proficiency will not be accepted.
- Other acceptable providers of language proficiency testing include the following professional interpreter associations: (The list is provided for informational purposes only and does not constitute FEMA's endorsement of any of the associations.)
  - American Translators Association (ATA)
  - American Council of Teachers of Foreign Languages (ACTFL) Bay Area Court Interpreters
  - California Court Interpreters Association California Federation of Interpreters, Inc. Educational Testing Services (ETS)
  - National Association of Judiciary Interpreters & Translators Northern California Translators Association
  - Southern California Translators Association Translators and Interpreters Guild

Language proficiency testing by colleges, universities, and additional institutions/associations may be accepted based upon FEMA's verification of an entity's credentials to conduct such tests.

When translations need arise, the Government will provide a completed form detailing the needed translations work. The Contractor will review the form and provide a quote for the requested services. The Government PM and COR must review the quote and approve the work prior to any translations work.

1. Foreign Language Translations

The Contractor shall provide foreign language translators to translate written, electronic and/or multi-media material from English to Spanish, Chinese (Simplified), Chinese (Traditional), Vietnamese, Korean, and Navajo languages. Other languages can also include but are not limited to French, Japanese, Tagalog, Arabic, Russian, Haitian (Creole), Portuguese, or braille. The Contractor should assume that the government's translation priorities shall evolve throughout the PoP.

Deliverable 3.C.1: Translations [As Assigned]

2. 508 Compliance and Desktop Publishing

The Contractor should meet the minimum personnel qualification requirements including current certification as a DHS Trusted Tester for 508 compliances.

ICPD also requires that the Contractor is up to date on scoping and technical requirements for information and communication technology (ICT) to ensure accessibility and usability by individuals with disabilities. Compliance with these standards is mandatory for Federal agencies subject to Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d).

The Contractor should also ensure that the translated work is complete with desktop publishing in order to align the translated work with the formatting of the original work which should include graphics or images associated with the work.

Deliverable 3.C.2.1: 508 Compliance [As Assigned]

Deliverable 3.C.2.2: Desktop Publishing [As Assigned]

3. Transcription / Captioning

ICPD requires transcription services of converting speech from audio/video sources or other formats into a written or electronic text from English to other languages. The Contractor shall provide services in all of the prioritized six languages listed in the scope and have the capability to provide transcription from English to other languages, if needed.

The Contractor shall be able to provide translators to perform scalable services in case there is a need to pick and choose particular sections from FEMA websites and publications.

Deliverable 3.C.3: Transcription / Captioning [As Assigned]

4. Website Localization

ICPD requires translations of FEMA websites from English to other languages. The Contractor shall provide services in all of the prioritized languages (Spanish, Chinese [Simplified], Chinese [Traditional], Vietnamese, Korean) and have the capability to provide translations in other languages.

The Contractor shall be able to provide translators to perform scalable services in case there is a need to pick and choose particular sections from FEMA websites.

Deliverable 3.C.4: Website Localization [As Assigned]

5. Voiceovers

ICPD requires voiceovers for animated video sources or other formats that have been transcribed and translated from English to other languages. The Contractor shall provide voice actors who can voice the script in the selected language. The Contractor should make sure that quality assurance is in place to confirm the timing of the translated script aligns to the timing of the English source script and can confirm the accuracy of the translation and quality of expression.

Deliverable 3.C.5: Voiceovers [As Assigned]

To help ensure accurate translations, the Government may prescribe specific validation measures (detailed below) in which the original translator must not participate. The Government reserves

the right to return to the Contractor all materials, transcriptions, and translations that contain errors at no additional cost to the Government. Upon receipt of "Requests for Correction," the Contractor will correct all errors and furnish corrected versions as required by the Task Monitor within five (5) working days. A complete and error free product is expected at the termination of each project. The Contractor shall provide either a summary of changes or a revised product with tracked changes.

Upon submission of completed translations, the Contractor shall be able to provide a report that provides evidence of a secondary review of the translated products to validate the accuracy of the translations. In this summary report, the Contractor will need to demonstrate that all translations have undergone a systematic process that shows a thorough review and proofreading of the translated products for quality assurance.

On a case-by-case basis, typically for high priority products, ICPD may require a Back Translation in order to fully validate the translation content. In this, a translated product is then translated back into the original source language (English). The back translations should be performed by (at least) two independent, separate translators who have not seen the original source document or material.

D. Conference and Partnership Management (T&M)

ICPD conducts various partnership and engagement activities to promote preparedness and preparedness resources. For example, ICPD staff may attend conferences and staff a booth that provides materials to other conference attendees. Upon request, the Contractor shall provide support for partnership and engagement activities. The support may include, but is not limited to, the following:

- Identifying conference and other engagement opportunities;
- Identifying and analyzing potential partnerships;
- Assisting with the development of a conference strategy;
- Building and maintaining logistics checklists for conferences;
- Preparing conference booth packages;
- Providing on-site conference or activity support; and
- Providing conference outcome analysis;

4. Task 4: Research, Analysis, and Evaluation

Due to the various factors involved in conducting research, analysis, and evaluation, costs for these projects will be based on Time and Materials (T&M). For each of these sections, Government program managers (PM) will develop task plans and work with Contract and Division leadership to develop and approve task budgets.

A. National Household Survey on Disaster Preparedness (T&M)

The National Household Survey on Disaster Preparedness (NHS) is a survey of the Nation's preparedness posture that assesses the public's perceptions, intentions, and behaviors related to disaster preparedness. The NHS provides practitioners with actionable information that can inform their decisions about how to promote preparedness and build capacity to respond to

disasters in their communities. The results are also used for performance metrics reported to FEMA and DHS and may inform programmatic decision-making.

Recent surveys included roughly 7,500 respondents, were entirely web-based, and were available in both English and Spanish. Future surveys may leverage a mixed-mode data collection approach using a combination of web, phone, and mail surveys and will be used to drive agency programmatic decision-making. Depending on approach, data collection may be considered T&M or an ODC.

Specific deliverables for this task will be prescribed in a task plan when exercised.

1. Data Collection and Analysis

The Contractor shall conduct the National Household Survey on Disaster Preparedness to measure the public's attitudes, actions, and beliefs towards disaster preparedness. This survey requires highly skilled experts in research, behavioral science, survey data analysis, as well as experts in developing and conducting surveys. In addition to key personnel for this task, the Government reserves the right to review, vet, and approve sub-contract support. The Contractor, along with any sub-contract support, should have proven experience conducting surveys in underserved and underrepresented communities.

Typical product, deliverables, and activities include, but are not limited to, the following:

- Survey Protocol to include objectives, target population, study design, sampling plan, collection plan, analysis plan, survey instrument, etc.
- Data collection
- Data cleaning and weighting
- Data analysis
- Data workbook
- Public summary of key findings
- Analysis syntax
- Methodology report
- OpenFEMA data package

Deliverable 4. A.1 NHS Data Collection and Analysis Package (per iteration of the NHS)

2. Outreach

The Contractor shall support the government with outreach communications to publicize the findings from the National Household Survey on Disaster Preparedness throughout FEMA and externally to emergency managers, academics, and the public. The Contractor shall produce two articles and a webinar script as promotional materials for each iteration of the National Household Survey on Disaster Preparedness.

Deliverable 4. A.2 NHS Promotional Package [per iteration of the NHS]

B. Analysis and Evaluation (T&M)

ICPD has a variety of portfolios and programs many of which collect data. For example, some programs have survey data which needs analysis to identify strengths and gaps of the programs. Program analysis should result in recommendations to enhance program delivery and efficiency.

In addition to ICPD programs, ICPD aims to promote and analyze the inputs from the Individual and Community Preparedness Learning Agenda. The Contractor shall provide support for collecting and analyzing stakeholder contributions to the Learning Agenda. In each PoP, the government PM will provide a task plan that prescribes the deliverables for this task.

C. Surveys (T&M)

The Contractor shall provide targeted surveys to test the impact of outreach messaging, training, exercises, and/or disaster survivor experiences in actual events. Targeted surveys may be for specific populations, geographic areas, or to gauge the effect of timely information. All surveys shall be conducted in conjunction with strategic efforts for increasing citizen awareness, knowledge, and skills and typically have a minimum of 500 respondents. The Contractor will work closely with the government PM and will develop budgets, create research protocols, conduct the research activities, perform the analysis, and report findings. In each PoP, the government PM will provide a task plan that prescribes the deliverables for this task.

D. Focus Groups (T&M)

The Contractor shall provide focus group capabilities to test the impact of outreach messaging, training, exercises, and/or disaster survivor experiences in actual events. Focus groups typically have a minimum of 20 respondents, unless otherwise required by the Paperwork Reduction Act (PRA). The Contractor will work closely with the government PM and will develop budgets, create research protocols, conduct the research activities (sometimes outside of regular business hours), perform the analysis, and report findings. In each PoP, the government PM will provide a task plan that prescribes the deliverables for this task. The Contractor, along with any sub-contract support, should have proven experience conducting focus groups in underserved and underrepresented communities.

E. Cognitive Testing (T&M)

The Contractor shall provide cognitive testing capabilities to test the impact of outreach messaging, training, exercises, and/or disaster survivor experiences in actual events. Cognitive testing groups typically have a minimum of 20 respondents, unless otherwise required by the Paperwork Reduction Act (PRA). The Contractor will work closely with the government PM and will develop budgets, create research protocols, conduct the research activities, perform the analysis, and report findings. In each PoP, the government PM will provide a task plan that prescribes the deliverables for this task.

F. Focused Interviews (T&M)

The Contractor shall provide focused interview capabilities to test the impact of outreach messaging, training, exercises, and/or disaster survivor experiences in actual events. In addition, interviews may focus on key informants for research or mission-specific needs. Interview studies

typically include 5-10 initial interviews and may also include follow-up interviews as needed unless otherwise required by the Paperwork Reduction Act (PRA). The Contractor will work closely with the government PM and will develop budgets, create research protocols, conduct the interviews, perform the analysis, and report findings. In each PoP, the government PM will provide a task plan that prescribes the deliverables for this task. The Contractor, along with any sub-contract support, should have proven experience conducting focused interviews with participants with limited English proficiency.

5. Task 5: Other Direct Costs

A. Materials (NTE)

The Contractor shall be allowed to direct charge cost for direct materials required in support of the overall mission task performance to include the following representative activities/items: offsite printing/copying/binding of briefings, reports manuals, color graphics, express/priority mailing/shipment, rental/purchase of presentation material/facilities/equipment to support meetings and seminars, or deployed/deploying systems, miscellaneous items to support system testing/training and operational readiness, Offsite facilities to support government meetings such as audio visual support, telephone support/conference calling/ VTC support. The Contractor shall be able to direct charge the cost for data collection, participation in meetings/seminars, conferences, and securing mission required equipment and hardware necessary to perform unique missions. In addition, the contractor shall direct charge for subscriptions to online tools as needed. Examples could include Survey Monkey, EndNote, Miro, and Kahoot.

Deliverable 5.A.1 ODC Materials [as needed NTE $20,000]

B. Printing (NTE)

The Contractor may be tasked to print materials under urgent circumstances when the GPO process is not feasible due to time constraints. All material must meet FEMA's Office of Disabilities printing requirements. The Contractor shall submit a minimum of three quotes from vendors for the requested work. The COR will review quotes and select/authorize the Contractor to use a vendor based on meeting the requirements and price. The funding for this deliverable will be determined near the end of each PoP and will be based on projection of unused contract funds. Printed materials must be delivered to prescribed locations by the end of the PoP.

Deliverable 5. B.1 ODC Printing [as needed NTE $50,000]

C. Travel (NTE)

1. Contractor Travel

The Contractor shall provide 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. Other travel destinations may include, Hawaii, Alaska, Puerto Rico, and any U.S. Territory.

When authorized as part of the scope of work and as *pre-approved by the 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 without a pre-authorization will not be reimbursed.

Travel requests must be submitted in sufficient time for the COR to give prior approval and must identify 1) the name of the traveler, 2) destination (s) including itinerary, 3) purpose of the travel, and 4) 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.

2. Invitational Travel

Every other year, the government will host a youth preparedness event. The Contractor will provide support with planning and logistics for the invitational travel as described in [add section here]. In addition, the government *may* opt to fund the invitational travel through the contract. This may include typical travel costs including, but not limited to air/rail/POV transportation, hotel, local travel, meals, and incidentals expenses (M&IE), etc.

G. Schedule of Deliverables

Deliverable 1.A.1	Project Management Plan (PMP) *[10 business days after Kick Off]*
Deliverable 1.A.2	Annual PMP Update *[10 business days after Option Year start]*
Deliverable 1.C.1	Monthly IPR Briefing *[NLT 10th business day of each month]*
Deliverable 1.C.2	Monthly Status Report *[NLT 5th business day of each month]*
Deliverable 1.D.1	Weekly Status Report *[Weekly]*
Deliverable 1.D.2	Weekly Budget Report for T&M Tasks *[Weekly]*
Deliverable 2	Program Updates *[three (3) annually]*
Deliverable 2.F.1	New Program *[as needed]*
Deliverable 3.A.1.1	Newsletter *[quarterly]*
Deliverable 3.A.1.2	News Blasts *[as assigned]*
Deliverable 3.A.2	Data Digest *[Up to 6 annually]*
Deliverable 3.A.3	Webinars *[as assigned]*

Deliverable 3.A.4.1	Weekly Case Management Report
Deliverable 3.A.4.2	Annual Case Management Report
Deliverable 3.B.1	Warehouse SOP Updates *[Two (2) per year]*
Deliverable 3.B.2	Stock Status Report *[weekly]*
Deliverable 3.B.3	Budget Report *[monthly]*
Deliverable 3.C.1	Translations [As Assigned]
Deliverable 3.C.2.1	508 Compliance [As Assigned]
Deliverable 3.C.2.2	Desktop Publishing [As Assigned]
Deliverable 3.C.3	Transcription / Captioning [As Assigned]
Deliverable 3.C.4	Website Localization [As Assigned]
Deliverable 3.C.5	Voiceovers [As Assigned]
Deliverable 4. A.1	NHS Data Collection and Analysis Package (per iteration of the NHS)
Deliverable 4. A.2	NHS Promotional Package [per iteration of the NHS]
Deliverable 5. A.1	ODC Salesforce Licensing and Materials *[NTE $230,000 Annually]*
Deliverable 5. A.2	ODC Webinar Software *[NTE $30,000]*
Deliverable 5. A.3	ODC Software Licensing *[NTE $40,000]*
Deliverable 5. B.1	ODC Printing *[as needed]*

H. General Contract Requirements and Project Management Techniques

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 contract:

- Technically proficient and professionally capable contractor personnel maintained throughout the life of the contract. The Contractor personnel must work collectively and professionally with any other ICPD contractors. The contractor personnel must maintain knowledge of Resilience/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 contract is continually monitored throughout the life of the contract.

- Provisions are made to add and/or remove contractor personnel as required by special tasks.

2. Quality Assurance and Continuous Improvement Program

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

3. Personnel

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

The Contractor is responsible for providing the necessary staffing with the requisite skill levels needed to accomplish the tasks. Contract personnel must meet specific qualifications and requirements. The minimum requirements may include education, experience, and certifications. Key Personnel must meet or exceed the requirements and any personnel changes must be approved by the COR. Non-Key Personnel changes will not need prior COR approval, but changes should be communicated in advance for planning purposes. Absences of Key personnel will be reflected in contract evaluations (e.g., CPARS). Any extended absences of non-Key Personnel adversely impacting contract performance will likewise be reflected in evaluations.

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 and other trainings.

A. Key Personnel

Program Manager

The Program Manager shall have full authority to act for the Contractor on all contractual matters relating to daily operation of this contract. A minimum of ten (10) years recent and relevant experience managing a contract of similar size and scope is required, including demonstrated experience managing the financials and budget projection in a contract of similar size. A bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred. Project Management Professional (PMP) certification is required. This position shall be on-site.

Task Leads (Program, Outreach, and Research, Analysis, and Evaluation)

The Task Leads (3) will manage the tasks under the direction of the Program Manager. A minimum of eight (8) years recent and relevant experience managing the subject task in a contract of similar size and scope is required. A bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred. Project Management Professional (PMP) certification is preferred, but not required.

Subject Matter Expert (SME), Preparedness

Subject Matter Experts (SMEs) (3) are technical experts called upon to provide assistance to ICPD on preparedness, communication, program, or project management, and other ICPD

initiatives as needed. SMEs shall have demonstrated knowledge of, and prior experience in, all applicable areas to requirements. A minimum of five (5) years of relevant experience is required. A bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred. The first two (2) personnel supporting the Task 2 Lead on Task 2 related work shall be Preparedness SMEs and are designated as Key for the FFP portion of work and their resumes shall be submitted with the proposal. The third SME will be added if/when needed, following standard Key Personnel approval procedures, and is considered non-key for the purposes of proposal submission for the T&M portion of work.

Behavioral Science Researcher

A Behavioral Science Researcher must have a minimum of 10 years' experience in behavioral sciences and research, as well as a Ph.D. from an accredited college or university OR 20 years' experience and Master's Degree from an accredited college or university. The researcher must be willing to travel a minimum of two weeks at any given time to any duty location within the Program Regions or Headquarters. This position will be essential to the success of this program.

Survey Researcher

A Survey Researcher must have a minimum of 10 years' experience in survey research and analysis, as well as a Ph.D. from an accredited college or university OR 20 years' experience and Master's Degree from an accredited college or university. The researcher must be willing to travel a minimum of two weeks at any given time to any duty location within the Program Regions or Headquarters. This position will be essential in completing tasks related to the National Household Survey.

Professional Writer/Copy Editor

Professional Writers/Copy Editors (1.5) must have proven professional work experience as a staff writer with a demonstrable portfolio of professional documents. Writer must be able to understand complex documents and translate into easily, consumable articles in plain English for public consumption. A minimum of five (5) years' experience and portfolio of work is required. The Professional Writer shall be able to write in styles consistent with the Chicago Manual of Style, Associated Press Stylebook, and the DHS standard style and branding. The Professional Writer will also be expected to adhere to FEMA's own style and branding guidelines. A bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred.

B. Non-Key Personnel

Jr. Analyst

Jr. Analysts assist others in performing functional duties with proper oversight. A minimum of three (3) years' relevant experience is required. A bachelor's degree from an accredited college or university is required.

Sr. Analyst

Sr. Analysts work on high visibility or mission critical aspects of given projects and performs all functional duties independently. A minimum of five (5) years' relevant experience is required. A

bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred.

Program Analyst

Program Analysts work on high visibility or mission critical aspects of given programs and performs all functional duties independently. A minimum of five (5) years' relevant experience in planning, executing, updating, and evaluating programs is required. A bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred.

Senior Research Analyst

Program Analysts work on high visibility or mission critical aspects of given programs and performs all functional duties independently. A minimum of five (5) years' relevant experience in research analysis is required. A bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred.

Program Support Specialist

Program Support Specialists work on high visibility or mission critical aspects of given programs and performs all functional duties independently. A minimum of five (5) years' relevant experience in program support is required. A bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred.

Communications Specialist

Communications Specialists work on public-facing outreach projects and initiatives. A minimum of five (5) years' relevant experience in drafting communications, maintaining relationships, drafting presentations and outreach material, and developing communications strategies is required. A bachelor's degree from an accredited college or university is required and master's degree from an accredited college or university is preferred.

Administrative Support Specialist

Administrative Support Specialists assist ICPD leadership to accomplish general administrative tasks. A minimum of three (3) years' relevant experience in preparing correspondence, receiving visitors, arranging conference calls, scheduling meetings, planning travel, and other administrative tasks is required. A bachelor's degree from an accredited college or university is required.

4. Business Hours

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

5. Telework

Telework, with FEMA authorized or issued equipment, is authorized under this order as approved by the COR. (i.e., working outside a government or contractor facility). Telework schedules and in person schedules will align with requirements for Federal staff. As of January

2024, the government requires four days of on-site presence every two weeks (four days per Federal pay period).

6. Performance of Period

The POP will consist of one (1) base period of seven (7) months and four (4) option periods each with a duration of 12 months.

- Base: 09/30/24 to 04/30/25
- OY1: 05/01/25 to 04/30/26
- OY2: 05/01/26 to 04/30/27
- OY3: 05/01/27 to 04/30/28
- OY4: 05/01/28 to 04/30/29

7. Government Furnished Equipment, Resources, and Facilities

The Contractor shall be responsible for completion of a site survey to identify any supplies and equipment that will be required by on-site personnel (up to six staff) for the successful completion of this PWS. Throughout performance of the contract, the Contractor shall identify any government furnished equipment (GFE) needs and submit request for approval and action by the COR.

The Government will provide the workspace, equipment, and supplies necessary to perform the on-site portion of Contractor services required in this contract, unless specifically stated otherwise in this work statement. Additionally, the Government will provide laptops and phones for contractor's working off-site. In total, FEMA will provide the following equipment for on and off-site Contractors to use in performing work under this contract.

- FEMA issued Laptops (up to 20)
- FEMA issued phones (up to 20)

The Contractor shall use Government furnished facilities, property, equipment and supplies only for the performance of work under this contract and shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear.

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

8. 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 contract; 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 contract 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 recipient 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 recipients 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 contract. Any continued future use of such DHS symbols by the vendor for its' own marketing of materials first developed under this contract, or other purposes beyond the life and purpose of this contract is strictly prohibited, unless permission is first requested by the vendor, and expressly approved in writing by the Contracting Officer.

9. Contractor Employee Identification

The Contractor shall comply with the requirements for Employment Eligibility Verification (Jan 2009), FAR 52.222-54. Contractor employees working on-site or visiting Government facilities shall wear an identification badge that, at 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 personnel shall identify themselves as Contractors in any telephone or e-mail communications when using Government equipment or systems. Contractors shall not present themselves as FEMA employees, but rather Contractors for FEMA.

10. Training

Child Safeguarding

Child Safeguarding means making all ICPD personnel and programs safe for children. ICPD requires that all Contractor employees who may support youth preparedness programming or interact with youth must complete FEMA's Child Safeguarding either synchronous or asynchronous training within two weeks of starting work on the contract, and before they interact with youth. The Contractor must then ensure that their employees stay up to date on their Child Safeguarding training according to the standard set by ICPD. This standard currently requires Child Safeguarding training be completed annually but may be subject to change in the future. The Contractor will work with the Child Safeguarding team to coordinate these trainings.

FAR 52.224-3 Privacy Training – Alternate I (DEVIATION 17-03) (July 2023)

(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 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(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.

11. Security

All personnel require access to information up to the sensitive but unclassified, for official use only (FOUO) levels. Contractor must ensure that all Contractor employees who required access to FEMA facilities and/or systems are U.S. Citizens and receive a favorably adjudicated public trust suitability prior to entry on duty (EOD). The Contractor shall follow the standards established within DHS and FEMA policy.

Unauthorized Disclosure of Classified or Unclassified Information:

Attachment 1

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

For Official Use Only (FOUO) Information:

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

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

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

Foreign Travel and Government-Issued Equipment

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

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

Background Investigations

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

Low Risk without Information System Access

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

Low Risk with Information System Access

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

Moderate Risk

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

High Risk

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

Background Investigation Process

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

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

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

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

FEMA PSD will only accept complete packages consisting of all of the above document and Standard Form 85P, which must be completed electronically through the Office of Personnel Management's e-QIP system. The Contractor is responsible for ensuring that all contractor personnel timely and properly submit all required background information.
Once contractor personnel have properly submitted the complete package of all required background information, FEMA's Personnel Security Division, at its sole discretion, may grant contractor personnel temporary eligibility to perform work under this contract prior to completion of the full background investigation if the Personnel Security Division's initial review of the contractor personnel's background information reveals no issues of concern. In such cases, FEMA's Personnel Security Division will provide notice of such temporary eligibility to the COR who will then notify the Prime Contractor, at which time the identified contractor personnel will be temporarily eligible to begin work under this contract. Neither the Prime Contractor nor the contractor personnel has any right to such a grant of temporary eligibility. The grant of such temporary eligibility shall not be considered as assurance that the contactor personnel will remain eligible to perform work under this contract upon completion of and final adjudication of the full background investigation.

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

Continued Eligibility and Reinvestigation

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

Exclusion by Contracting Officer

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

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.

12. Safeguarding of Sensitive Information (June 2023)

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

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

made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

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

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

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

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

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

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

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

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

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A (v13.3) dated February 13, 2023.
(3) DHS Security Authorization Process Guide
(4) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(5) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(6) DHS Information Security Performance Plan (current fiscal year)
(7) DHS Privacy Incident Handling Guidance
(8) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(9) 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
(10) NIST Special Publication 800-88 Guidelines for Media Sanitization

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

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A (v13.3) provides the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01- 007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.
(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.
(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

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

(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 13.3, February 13, 2023), or any successor publication and the Security Authorization Process Guide including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, http://csrc.nist.gov/publications/PubsSPs.html. Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment

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

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

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

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

(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least

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

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

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

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

(6) *Federal Reporting Requirements*. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall

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

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery. 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 attachments to email must be password protected. 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. Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;

(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

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

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

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

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

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

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

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

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

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

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

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

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

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

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

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

13.Privacy

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.

Attachment 1

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.

14. 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.

15.Section 504 and 508 Accessibility Requirements

SECTION 504 REQUIREMENT

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

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

SECTION 508 REQUIREMENT

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

16. Records Management Obligations

A. Applicability

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

B. Definitions

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

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

C. Requirements

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act

(FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

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

4. FEMA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of FEMA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to FEMA. The agency must report promptly to NARA in accordance with 36 CFR 1230.

5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the SOW. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to FEMA control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the SOW. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and FEMA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

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

8. The Contractor shall not create or maintain any records containing any non-public FEMA information that are not specifically tied to or authorized by the contract.

9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

10. FEMA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which FEMA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

17. 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.

18. Contractor Responsibilities

To accomplish the tasks outlined under this contract, the contractor will have access to the following PII: Name and business contact information, including: phone number, email addresses, and work addresses.

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 will ensure no computer matching, as that term is defined in 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 of 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.

19. DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.

- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Architecture Division (EAD) for review, approval and insertion into the DHS Data Reference Model and Mobius.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

20. Cyber-Supply Chain Risk Management

a. The Offeror understands and agrees that the Government retains the right to cancel or terminate the Contract, if the Government determines that continuing this solicitation presents an unacceptable risk to national security.

b. "Gray-Market" Equipment

   i. The Offeror shall provide only new equipment unless otherwise expressly approved, in writing, by the DHS Contracting Officer. Offerors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

   ii. The Offeror shall be excused from using new OEM (i.e., "gray market", "previously used") components only with formal Government approval, in writing, from the DHS Contracting Officer. Such components shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

   iii. All equipment obtained by the Offeror on behalf of the Government will need to be provided to OIG OCIO for review to validate requirements and approved Contractors by DHS.

c. Hardware and Software Requests

   i. The contractors supply the Government hardware and software will provide the manufacturer's name, address, state, and/or domain of registration, and the DUNS number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNS number of those suppliers must be provided.

ii. Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors will perform due diligence to ensure that these standards are met.

iii. The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

1. For software products, the Offeror shall provide all OEM software updates to correct defects for the life of the product (i.e., until the "End of Life (EoL)"). Software updates and patches shall be either: made available to the government for all products procured under this Contract, replaced upon End of Support (EoS) is reached, or formally waived (in writing) by the DHS Contracting Officer.

d. Supply-Chain Transport

i. Offerors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill Contract obligations with the Government.

ii. All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the Contract, the period of performance, or one calendar year from the date the activity occurred.

iii. This transit process shall minimize the number of times in route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

iv. All records pertaining to the transit, storage, and delivery shall be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

v. The Offeror is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government.

vi. The Offeror shall provide a packing slip which shall accompany each container or package with the information identifying this solicitation number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

vii. The Offeror shall send a shipping notification to the intended government recipient; with a copy transmitted via email to the Contracting Officer, or designated representative. This shipping notification shall be sent

electronically and will state this solicitation number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Notifications

i. The Offeror shall notify DHS Contracting Officer, COR and the Office of the Chief Information Officer and the DHS component Chief Information Officer through the Enterprise Security Operations Center (ESOC) directly of any suspected or potential violations of Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT) at NDAA_Incidents@hq.dhs.gov.

f. Foreign Equities

The Offeror shall immediately notify the DHS Contracting Officer, COR that will report to the Office of the Chief Security Officer (OCSO) or cognizant component personnel security office regarding any changes to corporate foreign ownership, control, or influence.

21.HSPD-12

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to DHS facilities, networks, and information systems. Personal Identity Verification (PIV) credentials shall be used as the primary means of logical authentication for DHS sensitive systems. The Contractor must use his or her federal issued Personal Identity Verification (PIV) credentials to access DHS resources to include IT applications and physical facility.

The DHS Office of the Chief Security Officer shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued Personal Identity Verification (PIV) credentials/identification cards and building passes that have either expired or have been

collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, 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.