Federal Emergency Management Agency

FEMA

STATEMENT OF WORK (SOW) FOR:

Phase 2: University Direct Technical Assistance (DTA) Network Project

[redacted] Contracting Officer

Revised August 12, 2024

Attachment A

DEPARTMENT OF HOMELAND SECURITY (DHS)

Date of Award: September 30, 2024

Statement of Work (SOW)

1.0 GENERAL

1.1 BACKGROUND

FEMA's Building Resilient Infrastructure and Communities (BRIC) Direct Technical Assistance (DTA) seeks to obtain contractor support to continue to expand the concepts of the University DTA Network, that was developed in Phase 1 under a contract with the Coastal Resilience Center (CRC) through a Basic Ordering Agreement (BOA) with the Department of Homeland Security Science and Technology (DHS S&T).

The general purpose of this work is to support the BRIC program in providing DTA to increase the capacity and capabilities of disadvantaged communities nationwide through the FEMA Hazard Mitigation Assistance (HMA), BRIC Program. As mentioned, this work is intended to move work performed in Phase 1 of identifying the capability and capacities of universities to support BRIC DTA, to continuing the development of a University DTA Network, including the development of a training program that will assist with a unified delivery of DTA from prospective university network members and DTA providers from across our other networks. Lastly, we seek evaluation of the network and the training program.

This project will enable the FEMA BRIC program to enable low-capacity communities to increase disaster resilience, improve mitigation outcomes, and foster capability and capacity building to reduce disaster suffering and costs, and address inequitable risks certain communities face. In most cases, this technical assistance will lead to future mitigation projects that can be implemented directly by tribal, state, and local governments.

This current presidential administration has prioritized work to support projects, especially in underserved communities, that emphasize the importance of technical assistance working across federal government and with external stakeholders. FEMA's Office of Resilience Strategies and Hazard Mitigation Directorate are looking to provide direct, coordinated, and place-based assistance and capacity building to ensure that disadvantaged communities can access and deliver generational resilience and infrastructure investments.

1.2 SCOPE OVERVIEW

Research and practice-based evidence has shown that many communities are struggling to effectively identify, develop, implement, and manage BRIC grants, particularly when compared

to larger and wealthier communities. The purpose of this effort is to further advance the concept and implementation of the University DTA Network. The network will harness the capabilities of the U.S. university and institutional systems and help advance the capacities of DTA communities and tribal nations. The University DTA Network will provide a framework for universities to join and learn from, while supporting the community of practice for resilience across the country.

1.3 OBJECTIVE

The objective of the Phase 2 University DTA Network Project is to continue the work from Phase 1 and move toward an evolved framework that can support universities delivering BRIC DTA needs. There will be tasks that include the continued identification and recruitment of potential University Network members. These members will be provided with a unified training program that will provide them with the tools to become subject matter experts in the delivery of BRIC DTA. These efforts will ultimately increase the overall resilience capabilities and capacities of the nation.

2.0 TASKS

2.1 PHASE 2 – TASKS

2.1.1 Continue to Develop and Enhance the University DTA Network

The primary tasks include the continued recruitment of potential university network members. The contractor will use information captured from Phase 1's identification of interested universities and begin to recruit them to be trained BRIC DTA capacity builders. This effort will not only support current BRIC DTA communities and tribal nations, it will also help FEMA build out national capacity and capability subject matter expertise that can support Hazard Mitigation Assistance for years to come. In addition, the contractor will continue to advance the idea of a sustainable University DTA Framework researched in Phase 1. This will include supporting the BRIC DTA team in maintaining a roster of universities identified and trained (through Task 2). It will also include continued support of developing on the ideas and proposed structure of what a University DTA Framework could be moving forward as identified within Phase 1. Ideas include a regional node concept, developing a network that is akin to the Agriculture Extension Offices and other models to be explored.

This task will build the foundational team of full-time dedicated staff to support the development of this project. This foundational team will support and recruit faculty, extension experts, and non-tenured faculty (professors of practice) to serve in the university network; manage the ongoing delivery of DTA training within the network and selected universities; assess and monitor the quality of that training; and help implement the university framework developed in Phase 1.

This team will serve as the foundation to support the sustainability of the network and provide the staffing needed to sustain and expand the network.

Potential roles could include the following:

Director, Deputy Director, Program Evaluation Coordinator, Recruitment, Training, Engagement, and Outreach Coordinator, Program Manager/Communication Coordinator, Direct Technical Assistance Advisor, Administrative Assistant, Grant Administrator, Graduate Students.

2.1.2 Develop and Deliver BRIC DTA Training Materials

Through our process of developing Phase 1 of this project and research identified through the development of the BRIC DTA Whitepaper for Cooperative Agreements, it was abundantly clear that there is a great need to develop unified BRIC DTA training materials. This task will deliver these training materials and provide an opportunity to test and evaluate the materials for improved delivery.

This funding will allow for the development of training materials and program needs based on feedback from the BRIC DTA team and Phase 1 recommendations. This training will be developed to align with existing FEMA training models but is geared toward providing specific guidance for University DTA Network participants and BRIC DTA providers. This task will support the development of a full-scale training program that any DTA provider can take to learn the FEMA approved DTA delivery. In addition, these materials will be used to support training needs for recipients of a Cooperative Agreement in the future, including specific focus on supporting universities work within the cooperative agreement being built by the FEMA BRIC program.

The content in the training program, will be based, in part, on input from FEMA (and their associated training materials and guidance), as well as targeted input from those interviewed in Phase 1 who successfully developed hazard mitigation grants in communities, and the results of the Phase 1 nationwide survey assessing capacity and commitment to BRIC grants management activities. University-specific topics identified in the Phase 1 interviews to be included in the training program include how to: 1) encourage university department chairs to support this type of work (versus just academic research and teaching); 2) assist university officials build local partnerships, to include how to engender trust; 3) recruit university partners to address gaps in university faculty knowledge; 4) engage students, recognizing their temporary job assignments; 5) incorporate classwork assignments into DTA assistance (i.e., data collection, field work, etc.); 6) partner with centers focused on disaster resilience; and 7) develop partnerships with MSI's. We will ask that the contractor to consolidate the large number of existing FEMA training courses and webinars into a set of discreet training modules focused on

BRIC DTA delivery.

We will ask that the contractor develop this training program to be transferable to the FEMA BRIC team and provide for a train the trainer type of delivery. The FEMA BRIC team will work with the selected contractor with selecting transferable deliver methods, such as training powerpoint templates, guides and materials used to develop the training and ways to deliver the training once complete.

Pilot training courses will be developed and delivered at locations to be identified and lessons/feedback will be collected to inform the final, FEMA-approved training course. During this task, the final FEMA approved training materials will be used and presented via webinars to University DTA Network members and DTA providers (including FEAM staff and contractors) in effort to support a unified message of delivering BRIC DTA across the nation and the support an on-going recruitment of University DTA Network members. The training task will be used to support the expansion of the network through supporting universities understanding of how to do business with FEMA, as well as supporting the community of practice for resilience within our university systems. In addition, the training will be delivered at select conferences where university faculty and extension officials involved in advancing disaster resilience are regular attendees. Potential conferences could include the following: 1) The Natural Hazards Workshop, hosted by the University of Colorado at Boulder; 2) The Higher Education Workshop at the Emergency Management Institute; and 3) the Extension Disaster Education Network Annual Conference. The training will need to be completed by university personnel and students within one calendar year of joining the University Network to remain eligible to be funded through the network to provide DTA assistance.

Furthermore, the training is intended to help create a community of practice. Historically, the provision of university assistance to assist underserved communities is highly variable, and in some cases is representative of an extractive process whereby faculty study communities without providing them useful information or assistance. Here a community of practice is intended to develop a more integrated, systemic assistance strategy that is of direct benefit to communities by enhancing their resilience. Given the training and university network involves students, the community of practice idea is multi-generational, and as students graduate, they may choose to work in this field as practitioners, government officials, and as university officials.

2.1.3 Evaluate the effectiveness of the University DTA Network and training program

The contractor will be tasked with evaluating the effectiveness of the University DTA Network and training programs developed in task 2. Steps to be taken will include the development of a performance evaluation program to measure University Network DTA process and outcomes. In addition, the contractor will be asked to update education and training materials based on the

results of the evaluation feedback produced from the performance evaluation program. The BRIC DTA team will work with the selected contractor to validate the performance evaluation program and the results produced.

2.1.4 Write Phase 2 Report Summarizing Findings, Lessons, and Next Steps

The contractor will write a report describing progress made to date, emphasizing identified milestones, issues identified, and solutions adopted. This information will be used to update and refine the framework developed in Phase 2. Specific elements in the Phase 2 report will include information derived from personal interviews with university network members who have attended the University DTA training. Interviews with identified university network members that have been trained will provide valuable insights in the future capabilities we could receive from universities participating in a Cooperative Agreement model. The report will conclude with recommendations developed by the contract team that span real time and long-term issues to improve the University Network-based DTA delivery process and training program.

9/1/24-9/1/25	
Tasks:	Completion Date
Task 1: Continue to Develop and Enhance the University DTA Network	September 2024 – August 2025
Task 2: Develop and Deliver BRIC DTA Training Materials	September 2024 – June 2025
Task 3: Evaluate the effectiveness of the University DTA Network and training program	January 2025 – August 2025
Task 4: Write Phase 2 Report Summarizing Findings, Lessons, and Next Steps	June 2025 – August 2025

3.0 CONTRACTOR PERSONNEL

3.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW.

3.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

3.3 Key Personnel

See Item 2.1.1 above.

3.3.1 CONTRACTOR KEY PERSONNEL SHALL NOT BE ASSIGNED BY THE CONTRACTOR TO MORE THAN ONE KEY POSITION FOR THIS REQUIREMENT.

3.4 Project Manager

The Contractor shall provide a Project Manager who shall be responsible for all Contractor work performed under this SOW. The Project Manager shall be a single point of contact for the Contracting Officer and the COR. It is anticipated that the Project Manager shall be one of the senior level employees provided by the Contractor for this work effort. The name of the Project Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Project Manager, shall be provided to the Government as part of the Contractor's proposal. The Project Manager is further designated as Key by the Government. During any absence of the Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. The Project Manager and all designated alternates shall be able to read, write, speak and understand English. Additionally, the Contractor shall not replace the Project Manager without prior approval from the Contracting Officer.

See Item 2.3.1.1. above.

3.4.1 THE PROJECT MANAGER SHALL BE AVAILABLE TO THE COR VIA TELEPHONE BETWEEN THE HOURS OF 8:00AM AND 5:00PM EST, MONDAY THROUGH FRIDAY, AND SHALL RESPOND TO A REQUEST FOR DISCUSSION OR RESOLUTION OF TECHNICAL PROBLEMS WITHIN 4 HOURS OF NOTIFICATION.

3.5 Employee Identification

3.5.1 CONTRACTOR EMPLOYEES VISITING GOVERNMENT FACILITIES SHALL WEAR AN IDENTIFICATION BADGE THAT, AT A MINIMUM, DISPLAYS THE CONTRACTOR NAME, THE EMPLOYEE'S PHOTO, NAME, CLEARANCE-LEVEL AND BADGE EXPIRATION DATE. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

3.5.2 CONTRACTOR EMPLOYEES WORKING ON-SITE AT GOVERNMENT FACILITIES SHALL WEAR A GOVERNMENT ISSUED IDENTIFICATION BADGE. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

3.6 Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

3.7 Removing Employees for Misconduct or Security Reasons

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

4.0 Other Applicable Conditions

This area should address other information the Contractor will need and/or requirements the Contractor will need to accomplish in the performance of the SOW. It is highly recommended that the topics included in SOW 4.1 through SOW 4.14 be addressed in the SOW. Additional topics may be added as appropriate.

4.1 Security

Contractor access to classified information is not currently required under this SOW. However, the Government later may require all Contractor personnel to have Secret clearances. Accordingly, all Contractor employees provided for this requirement must be eligible for a Secret Clearance.

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

Unauthorized Disclosure of Classified or Unclassified Information:

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

Access to the training can be obtained at:

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

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

OPSEC Training:

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

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

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

Insider Threat Training:

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

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

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.

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.

Conflict of Interest

The contractor shall take appropriate steps to ensure that neither the contractor nor any staff is placed in a position where, in the reasonable opinion of a neutral third party, there is or may be an actual conflict, or potential conflict, between the pecuniary or personal interests of the contractor and the duties owed to FEMA (or the prime contractor) under the provisions of the contract. The contractor will notify FEMA without delay giving full particulars of any such conflict of interest or appearance thereof which may arise.

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.

4.2 Period of Performance

The period of performance for this contract is for one-year period as follows:

Year One	September 30, 2024 through September 29, 2025

4.3 Place of Performance

The primary place of performance will be the Contractor's facilities with occasional visits to the Department of Homeland Security facilities in the Washington, DC Metro Area.

4.4 Hours of Operation

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

4.5 Travel

Travel may be required in the performance of the tasks described herein. No less than 21 days prior to any travel, the contractor shall submit an itemized cost estimate for the trip, covering all proposed attendees, including subcontractors, to the FEMA Contracting Officer's Representative (COR). The COR must pre-approve all travel. All travel costs associated with the execution of the tasks indicated in this SOW will be reimbursed in accordance with the limits set forth in the Federal Travel Regulations and the Federal Acquisition Regulations. Foreign travel is/is not allowed under this task order.

4.6 Post Award Conference

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 5 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held via teleconference.

4.7 Project Plan

The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 10 business days after the Post Award Conference. Project Management techniques will be memorialized in the plan to include delivery schedule, spending tracking and methods and recurring reporting on progress toward completion.

4.8 Business Continuity Plan

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 15 business days after the date of award, and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- How the Contractor will communicate with the Government during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
  - Telephone numbers
  - E-mail addresses

4.8.1 INDIVIDUAL BCPS SHALL BE ACTIVATED IMMEDIATELY AFTER DETERMINING THAT AN EMERGENCY HAS OCCURRED, SHALL BE OPERATIONAL WITHIN 4 HOURS OF ACTIVATION OR AS DIRECTED BY THE GOVERNMENT, AND SHALL BE SUSTAINABLE UNTIL THE EMERGENCY SITUATION IS RESOLVED AND NORMAL CONDITIONS ARE RESTORED OR THE CONTRACT IS TERMINATED, WHICHEVER COMES FIRST.

In case of a life-threatening emergency, the COR shall immediately make contact with the Contractor Project Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occur, the Contractor Project Manager and the COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- Essential Contractor work products expected to be continued, by priority

4.8.2 THE GOVERNMENT AND CONTRACTOR PROJECT MANAGER SHALL MAKE USE OF THE RESOURCES AND TOOLS AVAILABLE TO CONTINUE CONTRACTED FUNCTIONS TO THE MAXIMUM EXTENT POSSIBLE UNDER EMERGENCY CIRCUMSTANCES.

Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support ofauthorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

4.9 Progress Reports

The Project Manager shall provide a monthly progress report with accompanying metrics as to performance against schedule and budget to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

4.10 Progress Meetings

The Project Manager shall be responsible for keeping the COR informed about Contractor progress throughout the performance period of this contract, and ensure Contractor activities are aligned with DHS objectives. At a minimum, the Project Manager shall review the status and results of Contractor performance with the COR on a monthly basis via teleconference.

4.11 General Report Requirements

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

4.12 Intellectual Property

All contractor developed information and other forms of intellectual property developed under this Task Order (TO) shall be considered government property.

4.13 Protection of Information

Contractor will not have access to information protected under the Privacy Act is required under this SOW.

4.14 Section 508 Compliance

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

4.15 Privacy

To accomplish the tasks outlined in this contract, FEMA will share with the contractor the following PII data elements: Community names, Point of Contact (POC) Names (first and last), POC phone number, Business address of community, POC Email address.

The information sharing outlined in this contract is covered in the following Privacy Impact Assessment (PIA):

PIA: DHS/FEMA/PIA-025 Hazard Mitigation Grant Program (HMGP) System

Need to Know

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.

Prohibition on Computer Matching

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

Recipient Requirement

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 the 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.

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

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

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section

552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

including templates.

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

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

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

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

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

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

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

measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

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

(f) *Sensitive Information Incident Reporting Requirements.*

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

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

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

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

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

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

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

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

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

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

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

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

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

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

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

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

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

(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*.

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

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

Security Training Requirements.

All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later

than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

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

Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to

take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors.

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

employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e- mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

4.16 External Speaking Engagements

Pursuant to FEMA Directive 305-109, all requests for contractor personnel to speak on topics covered in this contract, in their official capacity, before non-federal entities or at forums attended by the public, are to be approved by the respective FEMA program office, Office of External Affairs (OEA), and the COR.

The contractor shall submit a partially completed FEMA Speaker Authorization Form to the COR. The contractor does not complete any portion of the Approval section. The COR will review with FEMA program staff and submit to the speaking engagement tool for review by OEA. OEA has 24 hours to bring up any concerns with the engagement. After that, it is sent to Office of Chief Counsel for legal review and clearance. If there is a deadline, please include that in the original submittal to the COR. If the content is not cleared timely, the COR and Program Office will determine if the contractor is permitted to present FEMA-related work at the speaking engagement.DHS Statement of Work (SOW)

5.0 Government Terms & Definitions

FAATBook_July2009_Web.indd (fema.gov) The Government will provide all necessary information, data and documents to the Contractor for work required under this contract.

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

6.0 Contractor Furnished Property

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in SOW 2.0 and SOW 6.0.

8.0 Government Acceptance Period

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

8.1 Invoices

Monthly invoices must be delivered to [INSERT EMAIL] with cc: to the COR and Contracting Officer listed below, no later than the 15th day of each month.

8.2 The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal.

In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

8.3 The COR will have 15 business days to review deliverables and make comments. The Contractor shall have 15 business days to make corrections and redeliver.

8.4 All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan.

The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

9.0 Deliverables

The Contractor shall consider items in BOLD as having mandatory due dates. Items in italics are deliverables or events that must be reviewed and/or approved by the COR prior to proceeding to next deliverable or event in this SOW. Invoices shall be tied to delivery and acceptance of products and services for the invoice period. Each invoice shall include sufficient detail to identify goods and services completed. In addition, each invoice shall detail the total charges by showing current and cumulative goods and services both currently invoiced and cumulative to date.

ITEM	SOW REFERENCE	DELIVERABLE/EVENT	DUE BY	DISTRIBUTION
1	4.6	Post Award Conference	5 business days from notice to proceed	N/A
2	4.7	*Draft Contractor Project Plan/Work Plan*	Day of the post award conference	COR, Contracting Officer, Project Monitor
3	4.7	Final Contractor Project Plan/Work Plan	10 business days from the post award conference	COR, Contracting Officer, Project Monitor
4	4.8	Original Business Continuity Plan	15 business days after the date of award	COR, Contracting Officer, Project Monitor
5	4.8	Updated Business Continuity Plan	Annually	COR, Contracting Officer, Project Monitor
6	4.9	Progress Reports	Monthly	COR, Contracting Officer, Project Monitor

ITEM	SOW REFERENCE	DELIVERABLE/EVENT	DUE BY	DISTRIBUTION
8	2.1.4	Annual Report	TBD	COR, Contracting Officer, Project Monitor