Statement of Work (SOW)
Federal Emergency Management Agency (FEMA)
Unarmed Security Monitors for Group Sites
DR-4673-FL
Within the State of Florida

1.0 GENERAL

This requirement is for Security Monitor's to provide service at all FEMA Group Sites constructed for DR-4673-FL in support of the Direct Temporary Housing Assistance Program. The Federal Emergency Management Agency (FEMA) shall use a local Security Company to provide all personnel, equipment and vehicles required to provide Security Services around the assigned group site.

1.1 SITE LOCATIONS

Security Monitor's shall support at the following Group Site location:

- **10660 Golden Journey Road, Fort Myers, FL 33908**

2.0 BACKGROUND

The Federal Emergency Management Agency (FEMA) uses unarmed security monitor services at federal government properties. Unarmed security monitors are being requested by some of the counties for safety of the sites in certain areas. Unarmed security monitor's the sites to make sure of no unwanted circumstances that take place day or night. Unarmed security consistently monitor's the assigned site and give daily surveillance, violations, and incident reports.

2.1 SCOPE

This requirement is for Unarmed Security Monitors to provide security services at disaster related group sites within the declared disaster area for DR-4673-FL in the State of Florida. All security personnel must also meet all local and state qualification requirements necessary to fulfill the responsibilities of the position.

2.2 OBJECTIVE

As an integral part of the FEMA security team, the Contractor shall provide and maintain all management, supervision, manpower, material, training, equipment, supplies, licenses, permits, certificates, insurance (vehicle), pre-employment screenings, reports, and files, and shall plan, schedule, coordinate and ensure effective performance necessary to accomplish security services as described and required in this Statement of Work (SOW). The Contractor is entirely responsible for timely obtaining and adhering to the individual state and city / municipality licensing and permits requirements without assistance from the Federal Government. The Contractor shall perform to the standards required in this SOW and will be expected to work closely with FEMA contracting and security representatives throughout the duration of services.

2.3 APPLICABLE DOCUMENTS

2.3.1 **Compliance Documents**

The following documents provide specifications, standards, or guidelines that must be complied with in order to meet the requirements of this contract:

- Federal Management Regulations (41 C.F.R. PART 102-74)
- American with Disabilities Act 9ADA) of 1990 (Pub L. 101-336)
- FEMA Directive 121-1, FEMA Personal Identity Verification Guidelines
- FEMA Directive 121-3, Facility Access
- FEMA Manual 121-3-1, FEMA Credentialing Access Manual
- Homeland Security Presidential Directive – 12
- DHS Management Directive 11042.1

2.0. SPECIFIC REQUIREMENTS/TASKS

2.1. GUARD POST ORDERS

The Contractor's employees shall perform the services as prescribed by the contract to include the Post Orders and security processes that are contained within the existing disaster Occupant Emergency Plan associated with the assignment.

In the event of an inconsistency or conflict between documents, the terms in this SOW take precedence over other documents.

2.1.1. Unarmed Security Monitors shall perform their duties in accordance with the duties outlined on the Post Orders, which are prepared by FEMA for all shifts. Except for emergencies, the responsibilities of the Unarmed Security Monitor may not deviate from the duties prescribed in the Post Orders. The COR may modify, amend, and/or revise Post Assignment Records to change shift duties, start and stop times, and post locations, provided the change has no impact on the contract cost. These changes will be issued in the form of new or updated post orders.

2.1.2. The duties of the guard posts require that an Unarmed Security Monitor not leave his or her post until properly relieved. Where this is required, it will be specifically stated in the Post Orders.

2.1.3. Changes to the post orders that increase or decrease the number of hours specified in the contract, or otherwise affect the contractor's cost or the contract price, will only be made by the CO.

2.1.4. Unarmed Security Monitor must be thoroughly familiar with the post orders at all posts where they are assigned to work. Whenever possible, Unarmed Security Monitor should be familiar with the Post Orders prior to working on the posts. When this is not feasible (i.e., when there are emergency nonrecurring services and the contractor is given limited advance notice regarding the Government's requirements), the contractor should allow, to the maximum extent practicable, Unarmed Security Guards mount time. Mount time is the period allowed for guards to prepare for the assumptions of their official duties, such as reading materials like post orders.

2.2. POST ASSIGNMENT

Post assignments may include, but are not limited to, the following duties and responsibilities:

2.2.1. Unarmed Security Monitor will be required to perform a variety of security-related duties. The post will have a Security Monitor Post Assignment Record (Post Orders). Specific duties and responsibilities associated with the post will be described in the Post Orders.

2.2.2. Unarmed Security Monitor must be thoroughly familiar with the Post Orders at the posts where they are assigned to work. Under no circumstance should any Unarmed Security Monitor neglect his/her assigned duties to familiarize him/herself with Post Orders.

2.2.3. Unarmed Security Monitor shall be knowledgeable of the site location and use of the nearest fire department, police station and hospital for group site emergencies (if any), and shall be ready, willing, and able to use them as necessary and as by the Post Orders (if it's with in contract standards).

2.2.4. Unarmed Security Monitor will be responsible for keeping logs and writing reports of incidents and occurrences encountered during their monitoring. At the end of each shift email reports of any non-incidents/incidents that occurs at the group site to FEMA POC and their supervisor.

2.3. ACCESS/EGRESS CONTROL

2.3.1. Unarmed Security Monitor will control access to the post area by observing, detecting, and reporting violations of post regulations as directed by the Post Orders

2.3.2. Unarmed Security Monitor shall monitor and report or call 911 of anyone attempting to gain unauthorized access to the property and/or personnel at the facility. Unarmed Security Monitor shall report all such incidents in accordance with established procedures as detailed in the Post Orders daily by emails.

2.4. SECURITY SCREENING

2.4.1. Unarmed Security Monitor shall monitor and report or call 911 of anyone attempting to bring prohibited or unlawful items into the property and/or personnel at the facility being monitored. Unarmed Security Guards shall report all such incidents in accordance with established procedures as detailed in the Post Orders

2.4.2. Unarmed Security Monitor shall be alert for unattended and suspicious packages. If the item is determined to be unattended or suspicious, Unarmed Security Monitor will call 911or notify the FEMA POC, if applicable. Unarmed Security Monitor will notify their supervisor of the incident and turn in a report to FEMA (email)

2.5. VISITOR PROCESSING

2.5.1. Unarmed Security Monitor will monitor visitors as directed in their Post Orders

2.5.2. Unarmed Security Monitor prior to arriving on duty, each Unarmed Security Monitor shall be familiar with the name, address, and location of his/her post, as well as the Post Orders of the assigned post.

2.6. MONITOR AND RESPONSE

2.6.1. Unarmed Security Monitor will monitor and report all suspected or apparent security violations by email

2.6.2. Monitored duties will be performed in a professional manner, with the Unarmed Security

Monitor responsible for observing the group site and reporting those persons whose activities arouse suspicion. Unarmed Security Monitor will monitor and report by email to FEMA POC and his/her supervisor to all emergencies occurring within the area of assignment

2.6.3. Unarmed Security Monitor must provide and maintain complete and effective surveillance, inspection, of all perimeter areas within the designated parameters and limits of the assigned post

2.6.4. Some posts may require a combination of fixed hours at a Unarmed Security Monitor site. Unarmed Security Monitor should adhere to the schedule as outlined in the Post Orders or as directed by the COR

2.6.5. Post hours are subjected to change with minimal notice from the Contracting Officer or the Contracting Officer's Representative (COR).

2.7. TRAFFIC CONTROL

When required by the Post Orders, Unarmed Security Monitor will monitor the environment for suspicious vehicles or persons. Unarmed Security Monitor may monitor and identify all suspicious vehicles as necessary to maintain a level of awareness to ensure the safety of all FEMA property and resources within the group site.

2.8. RULES AND REGULATIONS

Unarmed Security Monitor will familiarize themselves with Federal Management Regulations (41 C.F.R. part 102-74). Unarmed Security Monitor will monitor occupants and visitors for compliance with the Federal Management Regulations (41 C.F.R. part 102-74) and the group site posted rules and regulations. Unarmed Security Monitor shall monitor and report persons who violate the rules and regulations as appropriate and in accordance with and as directed by the Post Orders

2.9. EMERGENCIES

2.9.1. In case of an emergency condition requiring immediate attention, Unarmed Security Monitor shall call 911 and report in accordance with procedures in the Post Orders and at the direction of the COR. This may include diverting Unarmed Security Monitor from their posts to meet the condition and summoning appropriate assistance as may be required. Unarmed Security Monitor shall immediately make notifications as directed in the Post Orders

2.9.2. Unarmed Security Monitor shall report all move outs or empty units and items in need of repair, including inoperative lights, locks, security hardware, blocked emergency routes or exits, (visually be seen) etc.

2.9.3. Unarmed Security Monitor shall summon professional assistance in accordance with procedures in the Post Orders in the event of injury or illness to Government employees or others while on the grounds of a site

2.9.4. Unarmed Security Monitor shall prepare and maintain required reports in accordance with the Post Orders regarding security-related issues, such as accidents, fires, bomb threats, unusual incidents, and unlawful acts, and provide these reports to those officials specified by the COR

2.9.5. While on duty, Unarmed Security Monitor shall verbally report threatening circumstances and potentially threatening activities they observe to the COR or the onsite FEMA personnel. Whenever possible, Unarmed Security Monitor are encouraged to report a serious or potentially serious problem

before responding so that they may receive all necessary backup and support to lessen or eliminate the potential threat

2.9.6. Unarmed Security Monitor will be required to perform other such functions as may be necessary in the event of situations or occurrences such as civil disturbances, attempts to commit espionage, sabotage, or other criminal acts adversely affecting the security and/or safety of the Government, its employees, property, and the general public lawfully on the grounds under the control of the Government.

2.10. ASSIGNMENT AND SIGN-IN

2.10.1. The Contractor shall be responsible for scheduling all work and notifying Unarmed Security Monitor of their work schedules in a manner consistent with effective contract management.

2.10.2 When requested by the CO or COR, the Contractor shall furnish a copy of the most current schedule to the Government.

2.10.3. All Unarmed Security Monitor shall be in company uniform and ready to begin work promptly at the start of their shift and shall remain on the job and in full company uniform until the end of their full tour of duty.

2.10.4. The Contractor's employees shall sign in when reporting for work by (email) and shall sign out when leaving by (email) for FEMA records, on a DHS Form 139, Unarmed Security Monitor Duty Register. Monitor’s working overnight will sign out at 2400 and sign in at 0001 for billing purposes at the change of the calendar day.

2.10.5. Each successively lower line on DHS Form 139 must be completed in chronological order, without exception. Lines may not be left blank among signatures in any period. A single line entry shall be used when separating a calendar date.

2.10.6. Erasures, obliterations, superimposed or double entries of any type on any one line are unacceptable and will not be acceptable for payment purposes. If errors in signatures, times, post numbers, or duty status are made on the DHS Form 139, the next line, immediately below or following on subsequent sheet's lines containing such errors, will be used to record all information for every column in the correct manner. The contract employee should draw a single line through the entire line on which such mistakes appear. The Contractor must attach a detailed memorandum of explanation to each Form 139 containing erroneous entries for the purpose of correlating all mistakes made with the applicable valid lines of information, and for describing the reasons behind those mistakes. Payment of invoices is based on the above procedures.

2.10.7. The Contractor shall not remove the DHS Form 139s from the job site unless specifically authorized or instructed to do so by the CO or COR. The COR representative will collect all such forms. If the Contractor removes the DHS Form 139s from the post, payment may not be made until the original forms are received by the COR.

2.11. CONTRACT MODIFICATIONS:

The Contractor may be financially liable for accepting or implementing changes that affect the Contract price that have not been directed / approved by the CO. Therefore, the Contractor shall be responsible for verifying with the CO whether any requested changes should be provided pending issuance of a modification.

3.0. CONTRACTOR PERSONNEL

The Contractor shall provide qualified and approved personnel to perform all requirements specified in this SOW. Contractor will have a minimum (2) Security Monitor's as employees at the time of signing of the contract and be able to supply security monitors to posts under this contract for up to 12 hours per day.

3.1. MINIMUM QUALIFICATIONS

3.1.1. All Unarmed Security Monitor and Security Supervisors performing under the resulting contract/orders must meet the following minimum qualifications:

- U.S. Citizenship
- Proficiency in English (written and spoken)
- Current or prior security experience
- Have all state/local licenses, permits, registrations, or certifications as required to perform the duties and responsibilities of the position
- Must be at least 21 years of age

3.1.2. Use of Force Policy. Contractor must provide a copy of their company Use of Force Policy.

3.1.2. Work experience requirement. Each Unarmed Security Monitor shall have at least two years of security / police experience, or two years of military experience on active duty or in the National Guard or reserve military forces.

3.2. ESSENTIAL JOB FUNCTIONS

3.2.1. The Contractor shall ensure that all uniformed employees assigned to work under the Contract are in good general health without physical and/or psychological impairments that would interfere with the safe and efficient performance of their duties.

3.2.2. The Contractor is responsible for ensuring that all uniformed employees, both current and prospective, can perform the essential functions described below, with or without reasonable accommodation. If one of the Contractor's employees alleges that he/she has a disability and requires a reasonable accommodation to perform the essential functions of the job, it is the Contractor's sole responsibility to discuss reasonable accommodation, if any, to provide, at the Contractor's own expense.

3.2.3. The Contractor, not FEMA, is responsible for complying with the provisions of the American with Disabilities Act (ADA) of 1990 (Pub L. 101-336) and/or the Rehabilitation Act, as applicable, with respect to its employees.

3.2.4. All Unarmed Security Monitor's must be able to withstand the physical demands of the job and must be capable of responding to emergency situations without special accommodations by the Government.

3.2.5. The following are the essential job functions for uniformed employees working under the Contract:

- Work greater than 10-hour days and have the ability to work additional

hours due to unexpected activity.
- Work alone while unarmed.
- Frequent walking and sitting.
- Monitor and call 911 to life threatening or emergency situation.
- Any other related duties as determined by FEMA.

3.3. SUITABILITY

All Unarmed Security Monitor's and Security Supervisors must receive a favorable suitability adjudication from FEMA prior to beginning work under the contract.

3.4. FITNESS REQUIREMENTS

3.4.1. All contractor personnel who require access to DHS or FEMA information systems, 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.

3.4.2. The nature of the work performed by contract security guards, whether armed or unarmed, rises to the level of Public Trust High Risk.

3.4.3. Contractor personnel occupying positions or performing functions with a High-Risk designation shall undergo a background investigation and must receive a favorable adjudication thereof from FEMA PSD prior to performing work under this contract. The level of the background investigation will be determined by FEMA PSD.

3.4.4. Background Investigation Process

3.4.4.1. 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.

3.4.4.2. The Contractor shall also provide the FEMA COR with the following documents for each contractor personnel/applicant. The FEMA COR will ensure that all documents received are signed, dated, and witnessed as required prior to final acceptance and submission to FEMA Personnel Security along with the FF 121-3-1-6:

- Optional Form 306, Declaration for Federal Employment (OF306)
- Lautenberg Amendment Statement
- DHS Form 11000-6, Sensitive but Unclassified Non-Disclosure Agreement
- DHS Form 11000-9 (10/08) (FEMA edit 2017), Disclosure and Authorization
- And any other documents or forms required by FEMA PSD to complete the background investigation

- Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act.

3.4.4.3. 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:

3.4.4.3.1. The background investigation meets or exceeds the requirement of the contract position, and it was completed within the last five years,

3.4.4.3.2. The contractor applicant has not had a break in federal employment or federal contract employment since the prior favorable adjudication, and,

3.4.4.3.3. FEMA PSD has verified the investigation and confirmed that no new derogatory information has been disclosed which may require a reinvestigation.

3.4.4.4. FEMA PSD will notify the COR and the FEMA Security Manager at the specified work site 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.

3.4.4.5. For those contractor personnel who do not have an acceptable, prior, favorably adjudicated background investigation, 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"
- Standard Form 85P-S, "Supplemental Questionnaire for Selected Positions"
- Optional Form 306, "Declaration for Federal Employment"
- SF 87, "Fingerprint Chart" (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"
- Lautenberg Amendment Statement

3.4.4.6. FEMA PSD will only accept complete packages consisting of all of the above documents (Standard Forms 85P and 85P-S must be completed electronically through the Office of Personnel Management e-QIP system). FEMA PSD will notify the individual when and how to complete the Standard Form 85P and 85P-S. The Contractor is responsible for ensuring that all contractor personnel timely and properly submit all required background information.

3.4.4.7. 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 and the FEMA Security Manager at the specified work site. The COR will then notify the Contractor, at which time the identified contractor personnel will be temporarily eligible to begin work under this contract. Neither the 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 the completion and final adjudication of the full background investigation.

3.4.4.8. 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.

3.4.5. Continued Eligibility and Reinvestigation. Eligibility determinations 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.

3.4.6. 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.

3.5. CONTINUITY OF SUPPORT

The Contractor shall ensure that the contractually required level of support for this requirement is always maintained. 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.

The Contractor shall be responsible for providing a fully qualified replacement to meet all the requirements of the contract.

3.6. PROJECT MANAGER

The Contractor shall identify 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. 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. 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 and COR.

3.7. EMPLOYEE CONDUCT

3.7.1. 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 or FEMA uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees always present a professional appearance 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.

3.7.2. Unarmed Security Monitors are always expected to conduct themselves in an acceptable manner. While on post, Unarmed Security Monitor's shall refrain from:

3.7.2.1. Engaging in any disallowed activities while on post ex. non-official fraternization with applicants or visitors

3.7.2.2. Violating 41 C.F.R. part 102-74 subpart C or other Federal, state, or local law

3.7.2.3. Using any tobacco product

3.7.2.4. Using, watching, or listening to non-official audio or video devices

3.7.2.5. Sleeping, dozing, or napping

3.7.2.6. Playing cards or other games

3.7.2.7. The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, hygiene, appearance, and integrity, and shall be responsible for taking such disciplinary action with respect to its employees as may be necessary to include removal of a Contract Security Monitors from a contract at its own discretion or at the direction of the CO.

3.7.3 DHS and FEMA reserve the right and prerogative to deny and/or restrict the facility and information access, or to direct the removal from the Contract, of any Contractor employee who:

3.7.3.1. DHS or FEMA determines to present a risk of compromising sensitive Government Information to which he or she would have access to under this contract

3.7.3.2. Solicits or receives gifts based upon their contract position

3.7.3.3. Engages in personal use of government property

3.7.3.4. Uses government property or non-public information for private gain

3.7.3.5. Engages in political or private fundraising while on duty

3.7.3.6. Promotes or endorses political candidate or agenda while on duty

3.7.3.7. Engages in any inappropriate conduct while on duty

3.8. REMOVAL

The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to

remove any Contractor employee from DHS or FEMA facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract.

3.8.1. The COR may recommend to the CO that the CO direct the Contractor to remove any employee from any or all locations where the Contractor has contracts with the FEMA if the employee is not maintaining satisfactory performance in accordance with the contract.

3.8.2. The CO may direct the removal of employee for a disqualification for employment suitability, performance suitability, or security reasons, or found unfit for performing security duties during his/her tour of duty.

3.8.3. The CO may direct the removal of contract employees from the contract for misuse, willful damage, or willful destruction of Government property. The contract employee may face further penalties as deemed necessary by the Government.

3.8.4. In the event of a dispute by the Contractor of the directed removal, the CO will make the final determination.

3.8.5. The CO will provide specific reasons for removal of an employee to the Contractor in writing.

3.8.6. The Government shall not be responsible for any additional costs borne by the Contractor in connection with removed personnel.

4.0. OTHER APPLICABLE CONDITIONS

4.1. SECURITY REQUIREMENTS

4.1.1. 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:

4.1.1.1. Be aware of and comply with the safeguarding requirements for “For Official Use Only” (FOUO) information as outlined in this directive.

4.1.1.2. Participate in formal classroom or computer-based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information such as: Sensitive Security Information (SSI). SSI is a category of sensitive but unclassified information under the United States government's information sharing and control rules. SSI is governed by Title 49 of the Code of Federal Regulations (CFR), parts 15 and 1520. SSI is information that, if publicly released, would be detrimental to transportation security, as defined by Federal regulation 49 C.F.R. part 1520.

4.1.1.3. Understand that divulging information without proper authority could result in administrative or disciplinary action.

4.1.1.4. 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 or FEMA, but to whom access to information will be granted, may be requested to execute an N DA as determined by the applicable program manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

4.1.2. OPERATIONS SECURITY (OPSEC):
Contractors and Subcontractors who are working on this contract shall receive an OPSEC Awareness Brief. Access to the briefing can be obtained at http://cdsetrain.dtic.mil/opsec
Send the certificate of completion to the FEMA COR 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.

4.1.3. UNAUTHORIZED DISCLOSURE OF CLASSIFIED OR UNCLASSIFIED INFORMATION: The following language shall be incorporated in its entirety in the "Security" section of all requirement documents (Statement of Work, Statement of Objectives, or Performance Work Statement) establishing unauthorized disclosure of classified or unclassified information by contractors to perform duties established by the Government during the performance period of an executed contract:

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

4.2. PERIOD OF PERFORMANCE

The period of performance for this contract is a **PENDING** day base period with (XX) XXXXX day option periods as follows:

(6) months Base Periods

(2) Option Periods

4.3. PLACE OF PERFORMANCE

Although the specific site locations will vary, they will be within the State of "Florida". Locations will be specified in post assignments or verbally until followed up with a written post assignment.

The types of locations for which Unarmed Security Guards may be required include:

- Joint Field Offices (LIRO) and Annex
- Branch Offices
- Group Sites
- Disaster Relief Centers
- Mobile Disaster Relief Centers
- Logistical Staging Areas
- Responder Base Camps
- Temporary Housing Centers
- Annex offices
- Other facilities as identified by the on-scene FEMA Manager, as coordinated through the FEMA CO

4.4. HOURS OF OPERATION

Hours of operation will be specified in post assignments or verbally until followed up with a written post assignment. Limitation on Labor-hours to be provided by individual employees of the Contractor:

4.4.1. No employee of the Contractor or subcontracted employee shall provide more than twelve (12) hours of combined service on any one or multiple contracts administered by FEMA in any twenty- four (24) hour period, unless the work periods are separated by an eight (8) hour non-duty period.

4.4.2. The limitation on hours may be orally waived by the COR in emergencies that are beyond the control of the Contractor (i.e., weather conditions that prevent the next shift from getting to the facility, civil disturbances, natural disasters, emergencies, etc.). The Contractor shall provide the COR the written waiver request within 1 hour of identification of pending need. The COR will sign and return the wavier to the Contractor.

4.4.3. In no case shall any employee provide services under this Contract that exceed maximum allowed hours of service as set by applicable federal, state, or local law.

4.5. TRAVEL

Contractor travel shall not be required for this requirement and is not a reimbursable expense.

4.6. POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than one (1) business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held at the Government's facility, located at 1500 Main Street, Baton Rouge, Louisiana 70802, or via teleconference.

4.7. PROJECT PLAN

The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 30 days after the Post Award Conference.

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 30 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 two (2) 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 occurs, 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 of authorized 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 weekly progress report 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

4.10.1. 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 and FEMA objectives. At a minimum, the Project Manager shall review the status and results of Contractor performance with the COR monthly by phone or email.

4.10.2. The Project Manager shall also be available to meet personally with the COR monthly to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place at the JFO LA 1500 Main Street, Baton Rouge, Louisiana 70802

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 FEMA workstations (Windows 10 and Microsoft Office Applications).

4.12. CONTRACT TRANSITIONS

A smooth and orderly transition between the contractor and the Predecessor Contractor is necessary to assure minimum disruption to vital Contractor services and Government activities.

4.12.1. Phase-In of Contract and Continuity of Services

4.12.1.1. The Contractor shall not disrupt official Government business or in any way interfere

with the assigned duties of the predecessor Contractor's employees. The Contractor may notify the predecessor Contractor's employees that the Contractor will be assuming services upon the Contract start date and may distribute business cards, employment applications, brochures, and other company information to the predecessor Contractor's employees while they are on duty, provided that there is no interference with the Contract employee's assigned duties (e.g., during "off hours" or during relief or lunch breaks). However, the Contractor shall not interview, recruit, schedule interviews, or conduct extensive discussions with the predecessor Contractor's employee while they are on duty.

4.12.1.2. The Contractor shall provide a transition plan within five (5) working days after contract award. The transition plan shall include at a minimum all preliminary licensing and certifications required to initiate performance; process for transitioning predecessor employees; recruitment of new employees; and timeline showing procurement of requirement equipment and uniforms.

The Plan shall address:

- A strategy for implementing supervisory functions
- The process for transitioning predecessor employees
- Equipment inventory (radio & phone) and maintenance plan
- Weapons Inventory and employee assignment
- Communication plan
- Relief and break plan
- A plan for establishing a reserve force and the status of staffing levels,
- A progress report on obtaining permits, licenses, and registrations,
- A status report on submitting applications for personnel clearances,
- A strategy for training including schedules, locations, coordinating with training Contractors and class staffing
- The government will allow a seven (7) day start up from the time of the award of the base post assignment to the initial start of performance.
- The incumbent Contractor should cooperate to grant the employees release at a mutually agreed date.

4.12.2. Phase-Out of Contract and Continuity of Services

4.12.2.1. The Contractor shall provide a list with the total number of employees and their names performing on the Contract with any applicable suitability and certification expiration dates when requested by the CO in preparation for a new solicitation for follow-on services. Prior to Contract expiration, and after a follow-on contract is awarded, the Contractor shall exercise its best efforts and cooperation to affect an orderly and efficient transition to a successor contractor.

4.12.2.2 After a new Contract is awarded, the Contractor shall disclose necessary personnel records sufficient to allow the successor Contractor to conduct interviews for possible transition (if the Contractor is now awarded the successor Contract). These records shall be provided to the successor at least five (5) days prior to date of contract expiration. If any incumbent employees are selected by the successor and are agreeable to the change, the incumbent employees are selected by the successor and are agreeable to the change, the incumbent Contractor should cooperate to grant the employees release at a mutually agreed date.

4.12.2.3. As part of the closeout process, the Contractor shall, within 5 days of the final day of performance, turn over all incumbent officer training, suitability, and security records to the successor contractor. Failure to do so shall result in a 10% withholding of final payment until this action is accomplished as stated in the Contractor's Personnel Filing System.

5.0. GOVERNMENT TERMS & DEFINITIONS

Abbreviations Used Throughout the SOW:

- Department of Homeland Security (DHS)
- Federal Emergency Management Agency (FEMA)
- Contracting Officer (CO)
- Contracting Officer's Representative (COR)
- Contract Line-Item Numbers (CLIN)
- Continental United States (CONUS)
- Outside Continental United States (OCONUS)
- Law Enforcement Officer (LEO)
- Statement of Work (SOW)
- Office of the Chief Security Officer (OCSO)
- Field Operations Division (FOD)
- Personnel Security Division (PSD)
- Private Security Officer (PSO)

6.0. GOVERNMENT FURNISHED RESOURCES

The Government will provide copies of the references cited in SOW 1.4 at the Post Award Conference.

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.

7.0. CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish and maintain in acceptable condition all items of uniform and equipment necessary to perform work required by the Contract. The Contractor is solely responsible for the quality and performance of all Contractor-provided equipment used in performance of this Contract. The Contractor shall ensure that all uniformed personnel, including subcontractor employees, if any, are uniformed in the prime contractor's standard uniform. Contractor shall ensure that all employees' uniforms maintain a neat and organized appearance.

7.1. UNIFORM AND EQUIPMENT

- Shirts**: Company standard Issued S/Sleeve or L/Sleeve w/Company Shoulder Patches
- Pants: Company standard Issued - All weather
- Boots/Shoes: Company Standard
- Hat: Company Standard Baseball type with "Security" Imprinted
- Duty Belt with belt keepers
- Hand Cuffs w/ case
- Company Standard/Double lock Level II Firearm Retention Holster: Company Standard, Slide on Belt Type with Hammer
- Safety Strap: Left/Right as Required
- Double Magazine Case
- Weapon and Ammunition in accordance within this section
- Glove carrier/w latex gloves: Company Standard

- Expandable/Straight Police Baton w/ holder or Oleoresin Capsicum (OC) in 2.0-ounce Non- Flammable Flip Top Safety Canister with Fog/Cone, Stream, or Foam Spray Pattern with appropriate holster for container
- Patrol vehicles (4 x 4 vehicle when deemed necessary)
- Strobe lighting for the top of the vehicles
- All-terrain vehicles (when deemed necessary)
- Guard shack (when deemed necessary)
- Level II Ballistic Resistant vest

** Based on the time of year, geographic area and weather conditions, the Contractor along with the COR will decide what type of shirt is appropriate. A winter jacket, patrol type, may be required for the winter months; this will be determined by the Contractor and the COR.

7.2. FIREARMS AND AMMUNITION

7.2.1. No weapons are authorized in the performance of this contract.

7.3. SUPPLEMENTAL EQUIPMENT

7.3.1. The Contractor shall equip each guard post with supplementary equipment including, but not limited to:

- A notebook and pen.
- A serviceable, standard police-type flashlight of 700 lumens or more.

7.3.2. Contract Security Guards shall not possess any unauthorized supplemental or personal equipment (e.g., equipment not issued by the Contractor or required by the contract), such as privately owned (e.g., equipment not issued by the Contractor or required by the Contract) firearms, knives (except for a folding pocketknife), intermediate weapons, or other such nonstandard items. Contract Security Guards who are found in possession of such unauthorized equipment while on post shall face corrective action, such as forfeiture of the item(s), suspension, or permanent removal from the Contract.

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. REJECTION OF DELIVERABLES

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.

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.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	4.6	**Post Award Conference**		N/A
2	4.7	*Draft Contractor Project Plan*		COR, Contracting Officer
3	4.7	**Final Contractor Project Plan**		COR, Contracting Officer
4	4.8	**Original Business Continuity Plan**		COR, Contracting Officer
5	4.8	**Updated Business Continuity Plan**		COR, Contracting Officer
6	4.9	**Progress Reports**		COR, Contracting Officer
7				
8				
9				

10.0. CONTRACTING OFFICER REPRESENTATIVE (COR)

The Contracting Officer's Representative (COR) is a government employee appointed to assist the CO in the discharge of their responsibilities.

10.1. COR RESPONSIBILITIES The responsibilities of the COR include, but is not limited to:

10.1.1. Determining the adequacy of performance by the Contractor employees in accordance with the terms and conditions of this Contract Performing surveillance of the Contractor employees while they are on duty

10.1.2. Acting as the Government's representative in charge of work at the site

10.1.3. Ensuring compliance with Contract requirements insofar as the Unarmed Security Guards duties and behavior are concerned

10.1.4. Advising the Contractor and CO of non - performance or unsatisfactory performance

10.1.5. Other duties of the COR will be provided by the CO, if applicable.

10.2. APPOINTMENT LETTER

After award of the Contract, the CO will issue a written COR Appointment Letter specifying which Authority the CO is delegating to the COR or additional duties that they are authorized to perform. The COR cannot make any decisions regarding the performance of the Contract except as outlined in the letter. A copy of each letter shall be sent to the Contractor simultaneously upon issuance to the COR.

10.3. INSPECTIONS

The Government will use multiple means of inspection. FEMA will use its own announced and unannounced inspection and monitoring procedures in support of this Contract. Such procedures may occur at any time during the day or night, on any day of the year, and may be supplemented by FEMA’s customer surveys and other agency reviews of the Contractor’s performance.

11.0. CONTRACTOR OBLIGATION TO OBTAIN ALL REQUIRED LICENSES, PERMITS, AND BONDS

11.1. Prior to the Contract start date, and except were precluded by local law or ordinance, the Contractor shall make and complete all arrangements with the appropriate officials in the city, county, and parish, state and/or tribal in which the government facilities are located.

11.2. The federal government will not intervene in any state licensing or permit issues on behalf of the Contractor.

11.3. The Contractor shall obtain all licenses and permits required for each Unarmed Security Guard and Security Supervisor. Unarmed Security Guards must carry their firearm license and /permits (and, where legally required, their concealed weapons permit) on their person while on duty, unless local or state law requires the Contractor to maintain the records. Failure by a Unarmed Security Guard to carry a valid firearm certificate or permit while on duty shall result in the Contract Security Guard being removed from the post until the certificate or permit is obtained.

11.4. The Contractor shall provide any official bond(s) and insurance required, and pay any fees or costs involved or related to authorization for the arming of any employees engaged in providing services specified under the Contract.

11.5. The Contractor shall maintain current, valid copies of all licenses, permits, and certifications required to perform the services described in this SOW. The CO, COR, and all other authorized Government personnel shall have the express authority to examine these documents upon request at any time during the duration of this Contract. The Contractor shall complete and certify via email a spreadsheet showing employee compliance in accordance with contract policy within (7) days of the start of the contract. The spreadsheet shall reflect names and issue dates for each employee having each and all legally required licenses, permits, training and certifications as identified herein. The Contractor will validate and certify that the information on the spreadsheet is true and correct to ensure that all legal requirements have been fulfilled prior to the commencement of any and all work under the Contract.

11.6. The Contractor shall provide an updated spreadsheet to the Government upon the CO's or COR's request.

11.7. The Contractor shall obtain, possess, and maintain all business and corporate licenses required to operate as a commercial security service within the specific geographic areas covered under this the Contract prior to performing any work under the specific Contract.

<u>Important Note</u>: Failure by the Contractor to obtain all required licenses prior to the start of performance for the Contract may be grounds for termination for cause. Failure by the Contractor to renew licenses and permits upon their expiration may result in termination for cause. Failure by the Contractor to monitor licensing requirements of its personnel and immediately remove and replace any individual who for any reason does not have the required licenses may be grounds for termination for cause.

12.0. CONTRACTOR'S PERSONNEL FILING SYSTEM

To minimize duplication of effort by the Contractor, the Contractor shall maintain personnel files on-site for all employees who work under this Contract. Files shall be maintained at the Contractor's office and will be made available to the COR on a continuous basis. Each guard's file must contain the following:

- Application for employment, including resume or detailed prior work history and references.
- Driver's license/state identification
- Lautenberg amendment/domestic violence statement (annual)
- Results of all criminal history checks obtained by the Contractor.
- U.S. Citizenship and Immigration Services Form I-9 Employment Eligibility Verification (OMB No 1115-0136);
- A copy of DHS 11100-6 Non-Disclosure Agreement,
- A copy of high school diploma, GED certificate, college transcripts military records or POST training completion.
- A copy of the most recent CPR, First Aid, and AED certification card.
- Results of all drug screenings administered (both pre – and post – employment).
- A copy of all firearm licenses and certifications required by state and local requirements
- State Security Officer Certification (as required)
- Local permits and renewals (as required)

- Records of all basic and refresher training attendance and, where required test scores.
- Records of current firearms training and qualification scores, where required by the Contract.
- Current baton or OC certification
- Records of all successfully completed Government-provided training.
- Records of guard's suitability information (Including date current suitability expires).
- Copies of all complaints, investigations, and disciplinary action taken by the Contractor against the employee for all infractions committed under the contract.
- To comply with the Health Insurance Portability & Accountability Act (HIPPA), the Medical Evaluation (SF-78_ may be filed separately by the contractor

12.1. FILE REVIEW: The CO or COR shall have the express authority to review any Contract employee's files at any time during the Contract. The Contractor shall maintain all personnel files for a minimum of six (6) years after Contract closeout (upon receipt of release of claims).

12.2. TRACKING SYSTEM: The CO or COR can request, at any time during the course of the Contract, a spreadsheet or other tracking systems (either in paper form or in electronic form) that clearly details the status of all Contract employees pertaining to the Contract requirements, and all site locations within the contract.

12.2.1. The Contractor may maintain either a hard-copy (paper) file or a computerized system containing all the information required above. However, if the Contractor uses a computerized filing system, all forms must be scanned into the computer and must be legible.

12.2.2. False statements, certification, or falsification of any documents required in the Contract by the Contractor, Contract Manager or any Contract employee shall be punishable under US Code Title 18, Chapter 47 Section 1001, Fraud and False Statements. Additionally, the Government may initiate investigations by is Office of Inspector General or the FEMA Fraud Investigative Internal Division (FIID), may initiate debarment proceedings, and/or may take Contractual remedies up to and including termination for default. Under no circumstances whatsoever will the Government tolerate falsification of required documents.

12.3. FILE TRANSITION: After the award of a new Contract the outgoing Contractor shall provide personnel records, including, but not limited to training, medical, suitability, and security records to the incoming Contractor. The outgoing Contractor shall provide these records to the successor at least 45 days prior to date of contract expiration. The Government reserves the right to inspect all documentation provided to the incoming Contractor. Failure to provide all records to the successor Contractor as required may result in FEMA withholding of final payment until completion of this action and may negatively impact the outgoing Contractor's performance evaluation.

13. 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.

14. 508 INFORMATION TECHNOLOGY CLAUSE

https://www.dhs.gov/compliance-test-processes

DHS 508 Tool: https://www.dhs.gov/xlibrary/oast/DART/

Note: The 508 IT clause is generated from the DHS 508 Tool on an ad hoc basis.
The 508 IT clause generated from the DHS 508 Tool is inserted into the PWS or SOO or SOW.

Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 Telecommunications Products applies to all telecommunications products including end-user interfaces such as telephones and non-end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

36 CFR 1194.31 Functional Performance Criteria applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

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 COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

15. DHS ENTERPRISE ARCHITECTURE COMPLIANCE

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

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

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

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

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

(e) Applicability of 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.

[1] Department of Homeland Security (DHS) Directives System, *Enterprise Data Management Policy*, 2008. https://www.dhs.gov/sites/default/files/publications/mgmt_directive_103_01_enterprise_data_management_policy.pdf

16. 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:
(a) 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

(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*.

17. 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.

18. INFORMATION SHARING

Authorities: This information sharing, including the collection and dissemination of information described in this contract, is authorized by 5 U.S.C. § 301, the Homeland Security Act, codified in Title 6 of the U.S. Code; the DHS/ALL/PIA-039 Physical Access and Control System (PACS) (July 2019) and Routine Uses F and H of the DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 Fed. Reg. 5609 (Feb. 2010), Final Rule for Privacy Act Exemptions, 74 Fed. Reg. 42578 (Aug. 2009).

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

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

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.

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.

The above Information Sharing terms are to be considered collectively with the terms stated below in the sections SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015) and INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015).

********** END OF DOCUMENT **********