

Department of Homeland Security Federal Emergency Management Agency



Federal Emergency Management Agency

Performance Work Statement Level II-Armed Protective Security Officers

Indiana

Performance to be conducted in State of/Territory of **Indiana**.

The Vendor shall have **20** Level II Armed Protective Security Officers available at the start of the contract

The Period of Performance is base: **3 Months, and 3 Options of 3 Months**

Table of Contents

1.0. GENERAL

1.1. BACKGROUND

1.2 SCOPE

1.3 OBJECTIVE

1.4 APPLICABLE DOCUMENTS

1.5 PERFORMANCE REQUIREMENTS SUMMARY

2.0 SPECIFIC REQUIREMENTS/TASK

2.1 GUARD POST ORDERS

2.2 POST ASSIGNMENT

2.3 ACCESS/EGRESS CONTROL

2.4 SECURITY SCREENING

2.5. VISITOR PROCESSING

2.6 PATROL AND RESPONSE

2.7 TRAFFIC CONTROL

2.8 BUILDING RULES AND REGULATIONS

2.9 EMERGENCIES

2.10 ASSIGNMENT AND SIGN-IN

2.11 CONTRACT MODIFICATIONS

3.0 CONTRACTOR PERSONNEL

3.1 MINIMUM QUALIFICATIONS

3.2 ESSENTIAL JOB FUNCTIONS

3.3 SUITABILITY

3.4 FITNESS REQUIREMENTS

3.5 CONTINUITY OF SUPPORT

3.6 PROJECT MANAGER

3.7 EMPLOYEE CONDUCT

3.8 REMOVAL

4.0 OTHER APPLICABLE CONDITIONS

4.1 SECURITY REQUIREMENTS

4.2 PERIOD OF PERFORMANCE

4.3 PLACE OF PERFORMANCE

4.4. HOURS OF OPERATION

4.5. TRAVEL

4.6. POST AWARD CONFERENCE

4.7 PROJECT PLAN

4.8 BUSINESS CONTINUITY PLAN

4.9 PROGRESS REPORTS

4.10 PROGRESS MEETINGS

4.11 GENERAL REPORT REQUIREMENTS

4.12 CONTRACT TRANSITIONS

5.0 GOVERNMENT TERMS & DEFINITIONS

6.0 GOVERNMENT FURNISHED RESOURCES

7.0 CONTRACTOR FURNISHED PROPERTY

7.1. UNIFORM AND EQUIPMENT

7.2. FIREARMS AND AMMUNITION

7.3. SUPPLEMENTAL EQUIPMENT

8.0. GOVERNMENT ACCEPTANCE PERIOD

8.1. REJECTION OF DELIVERABLES

9.0 DELIVERABLES

10.0 CONTRACTING OFFICER REPRESENTATIVE (COR)

10.1 COR RESPONSIBILITIES

10.2. APPOINTMENT LETTER

10.3. INSPECTIONS

10.4 PERFORMANCE REQUIREMENTS SUMMARY (PRS)

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

12.0 CONTRACTOR'S PERSONNEL FILING SYSTEM

13.0 RECORDS MANAGEMENT OBLIGATIONS

14.0 508 INFORMATION TECHNOLOGY CLAUSE

15.0 DHS ENTERPRISE ARCHITECTURE COMPLIANCE

16.0 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION

17.0 INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING

Performance Work Statement (PWS)
Federal Emergency Management Agency (FEMA)
Level II Armed Protective Security Officers

1.0 GENERAL

1.1 BACKGROUND

The Federal Emergency Management Agency (FEMA), Office of Chief Security Officer, in accordance with the Robert T. Stafford Disaster Relief and Emergency Assistance Act, often called the Stafford Act, uses contracted Level II Armed Protective Security Officers to safeguard federal employees, visitors, and property at both temporary and fixed facilities during disaster and emergency declarations. Congress enacted the Homeland Security Act of 2002, Public Law 107-296, 116 Stat 2135 (Nov. 25, 2002) (the Act) to better protect the assets and critical infrastructure of the United States. The Act expressly transfers the authority for law enforcement and related security functions for Federal properties from the GSA to the Secretary of DHS. Level II Armed Protective Security Officers have a crucial and highly visible role in the FEMA mission.

The Act requires the Secretary to “protect the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed-ownership corporation thereof) and the persons on the property.” 40 U.S.C. 1315(a). The Act further authorizes the Secretary to designate officers and agents “for duty in connection with the protection of property owned or occupied by the Federal Government and persons on the property, including duty in areas outside the property to the extent necessary to protect the property and persons on the property.” 40 U.S.C. 1315(b)(1). Thus, in addition to moving the protective mission into DHS, the statute further expanded DHS's protective coverage to include duties in areas outside federal property to the extent necessary to protect federal property and persons thereon, as well as authorizing off-property investigations related to the protection of federal property and the individuals on that property. 40 U.S.C. 1315(b)(2)(E). To ensure a fast response to disasters an established Contract for Level II Armed Protective Security Officers will minimize the repetitive procurement process and ensure management and mitigation of any procurement, fraud, waste and abuse FEMA mission. They are usually the first line of defense, so it is crucial that the Contractor ensure that their employees realize the importance of their role, know their duties, and always perform their duties courteously and professionally.

- a. On Jan. 24, 2025, President Trump issued Executive Order 14180 establishing the Federal Emergency Management Agency Review Council (FEMA Review Council), noting “the need to drastically improve [FEMA’s] efficacy, priorities, and competence, including evaluating whether FEMA’s bureaucracy in disaster response ultimately harms the agency’s ability to successfully respond.”
- b. The Current Presidential Administration’s goal is to hold States accountability to the states on Mitigation, Response, and Recovery. The COUNCIL TO ASSESS THE FEDERAL EMERGENCY MANAGEMENT AGENCY was established January 24, 2025. The Council shall advise the President, through the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the Director of the Office of Management and Budget, on the existing ability of FEMA to capably and impartially address disasters occurring within the United States and shall advise the President on all recommended changes related to FEMA to best serve the national interest.
 - i. Reference: <https://www.whitehouse.gov/presidential-actions/2025/01/council-to-assess-the-federal-emergency-management-agency/>

1.2 SCOPE

This requirement is for Contract Level II Armed Protective Security Officers to provide security services throughout Indiana that is issued a major disaster declaration, primarily at disaster related sites

and facilities within the declared disaster. The requirement could occur in any county, throughout Indiana. The immediate requirement will be for armed guard services to be provided within 24 hours of the execution of Attachment 01 - Guard Task Order Form against the Contract. **The vendor shall have 20 Level II Armed Protective Security Officers** available at the start of the contract. The Program Office will then issue Attachment 01 - Guard Task Order Form for location, dates, and times to have the Level II Armed Protective Security Officers performance.

Other FEMA facilities could be open in other areas of the declared state which would require Level II Armed Protective Security Officers in facilities located in any or all counties throughout Indiana.

The Contractor may only utilize Department of Labor (DOL) category 27102 Guard II security personnel to perform services under this contract. All category Guard II security personnel must also meet all local and state qualification requirements necessary to fulfill the responsibilities of the position.

1.3 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, 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 Performance Work Statement (PWS). 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 PWS and will be expected to work closely with FEMA contracting and security representatives throughout the duration of services.

1.4 APPLICABLE DOCUMENTS

1.4.1 Compliance and Reference Documents

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

- 1.4.1.1 Attachment 02 - Federal Management Regulations (41 C.F.R. PART 102-74)
- 1.4.1.2 Attachment 03 - American with Disabilities Act 9ADA) of 1990 (Pub L. 101-336)
- 1.4.1.3 Attachment 04 - FEMA Directive 121-1, FEMA Personal Identity Verification Guidelines
- 1.4.1.4 Attachment 05 - FEMA Directive 121-3, Facility Access
- 1.4.1.5 Attachment 06 - FEMA Manual 121-3-1, FEMA Credentialing Access Manual
- 1.4.1.6 Attachment 07 - Homeland Security Presidential Directive – 12
- 1.4.1.7 Attachment 08 - DHS Management Directive 11042.1

1.5 PERFORMANCE REQUIREMENTS SUMMARY

This Contract includes a Performance Requirements Summary (PRS) at PWS 10.4. The PRS plays an integral role in the administration of the contract. In addition to any applicable inspection clauses or other related terms and conditions contained in the agreement, the PRS shall serve as a primary tool for inspection and acceptance of services as facilitated by the Contracting Officer's Representative (COR). Evaluation of the Contractor's overall performance shall be in accordance with the performance standards set forth in the PRS, and will be conducted by the COR. The PRS constitutes a material aspect of the contract and will not be changed or otherwise modified without prior written approval of the Contracting Officer.

2.0. SPECIFIC REQUIREMENTS/TASK

2.1. GUARD POST ORDERS

The Contractor's employees shall perform the services as prescribed by the contract, to include Attachment 01 - Guard Task Order Form, and Attachment 09 - Security Guard Post Assignment Record (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 PWS take precedence over other documents.

2.1.1. Level II Armed Protective Security Officers shall perform their duties in accordance with the duties outlined on the Post Orders which are prepared by FEMA for all shifts on each post. Except for emergencies, the responsibilities of the Level II Armed Protective Security Officers may not deviate from the duties prescribed in the Post Order 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 increased impact on the Contract cost.

2.1.2. The duties of some guard posts require that an Level II Armed Protective Security Officers 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, the amount of equipment and/or supplies required, or otherwise affect the Contractor's cost or the Contract price, must be made by the Contracting Officer (CO).

2.1.4. Level II Armed Protective Security Officers must be thoroughly familiar with the post orders at all posts where they are assigned to work. Whenever possible, Level II Armed Protective Security Officers 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, Level II Armed Protective Security Officers 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, loading and holstering the firearm, etc.

2.2. POST ASSIGNMENT

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

2.2.1. Level II Armed Protective Security Officers will be required to perform a variety of security-related duties, depending on the type of posts to which they are assigned. Each post will have a Level II Armed Protective Security Officers Post Assignment Record (Post Orders). Specific duties and responsibilities associated with each post will be described in the Post Orders.

2.2.2. Level II Armed Protective Security Officers must be thoroughly familiar with the Post Orders at all posts where they are assigned to work. Under no circumstance should any Level II Armed Protective Security Officers neglect his/her assigned duties to familiarize him/herself with Post Orders. Level II Armed Protective Security Officers shall be knowledgeable of the location and use of the nearest first aid kit, fire extinguisher, fire alarm, emergency exit, and duress alarm (if any), and shall be ready, willing, and able to use them as necessary and as required by the Post Orders.

2.2.3. Level II Armed Protective Security Officers will be responsible for keeping logs and writing reports of incidents and occurrences encountered during the tour of duty.

2.3. ACCESS/EGRESS CONTROL

2.3.1. Mount time is the period allowed for guards to prepare for the assumptions of their official duties, such as Level II Armed Protective Security Officers 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. Level II Armed Protective Security Officers shall prevent, discover, delay, and/or detain/persons attempting to gain unauthorized access to the property and/or personnel at the facility being protected. Level II Armed Protective Security Officers shall report all such incidents in accordance with established procedures as detailed in the Post Orders.

2.3.3. Level II Armed Protective Security Officers may be required to lock or unlock specific entrances/exits and turn on/off lights in their duty area at specific times as prescribed in the Post Orders.

2.4. SECURITY SCREENING

2.4.1. Level II Armed Protective Security Officers shall screen personnel, packages, and vehicles for prohibited or unlawful items using manual, automated, or integrated screening techniques.

2.4.2. Level II Armed Protective Security Officers shall prevent, discover, delay, and/or detain/person's attempting to bring prohibited or unlawful items into the property and/or personnel at the facility being protected. Level II Armed Protective Security Officers shall report all such incidents in accordance with established procedures as detailed in the Post Orders.

2.4.3. Level II Armed Protective Security Officers shall be on alert for unattended and suspicious packages. If the item is determined to be unattended or suspicious, Level II Armed Protective Security Officers will notify the FEMA Security Manager assigned. Level II Armed Protective Security Officers will notify in accordance with Attachment 09 - Security Guard Post Assignment Record (Post Orders), FEMA Contracting Officer Representative, designated person identified on site and their "Business Chain of Command."

2.5. VISITOR PROCESSING

2.5.1. Level II Armed Protective Security Officers shall process visitors as directed in their Attachment 09 - Security Guard Post Assignment Record (Post Orders).

2.5.2. Level II Armed Protective Security Officers are required to answer questions and provide directions to visitors and facility tenants. Prior to arriving on duty, each Level II Armed Protective Security Officers shall be familiar with the name, address, and location of his/her post, as well as the Post Orders of the assigned post. Each Level II Armed Protective Security Officers shall be familiar with each tenant Agency's name and the locations within the facility of the most commonly sought-after offices or locations, such as service offices, restrooms, elevators, entrances and exits, retail spaces, and parking areas, and shall provide that information to any visitor upon request.

2.6. PATROL AND RESPONSE

2.6.1. Level II Armed Protective Security Officers will conduct patrols in accordance with routes and schedules established in the Post Orders. They will observe, detect, report, and respond to all suspected or apparent security violations.

2.6.2. Patrol duties will be performed in a professional manner, with the Level II Armed Protective Security Officers responsible for observing the environment, and, when necessary, questioning those persons whose activities arouse suspicion. Patrol Level II Armed Protective Security Officers will serve as the first responder to all security alarms and emergencies occurring within the area of assignment. Level II Armed Protective Security Officers must provide and maintain complete and effective surveillance, inspection, and protection of all internal and perimeter areas within the designated parameters and limits of the assigned post. When applicable Level II Armed Protective Security Officers shall call 911 and report to law enforcement when observing criminal activity in progress.

2.6.3. Some posts may require the Level II Armed Protective Security Officer a combination of duties at the assigned post. These are fixed/static at a facility post and roving patrols. Level II Armed Protective Security Officers should adhere to the patrol schedule as outlined in the Post Orders or as directed by the COR.

2.6.4. Post hours are subjected to change with minimal notice at the beginning of the disaster.

2.7. TRAFFIC CONTROL

When required by the Post Orders, Level II Armed Protective Security Officers will direct traffic on government leased or owned property (vehicular and pedestrian) to include control parking and observe the environment for suspicious vehicles or persons. Level II Armed Protective Security Officers may operate traffic control points and identify, delay, and detain all-suspicious vehicles and personnel as necessary to maintain a level of security sufficient to ensure the safety and protection of all personnel, property, and resources within the FEMA or Federal facility. Suspicious vehicles and persons outside the facility shall be reported to law enforcement by calling 911.

2.8. BUILDING RULES AND REGULATIONS

Level II Armed Protective Security Officers will monitor and observe building occupants and visitors for compliance with the Attachment 02 - Federal Management Regulations (41 C.F.R. part 102-74) and the facility's posted rules and regulations. Level II Armed Protective Security Officers shall also identify, report, delay, or detain those persons/personnel 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, Level II Armed Protective Security Officers shall act in accordance with procedures in the Post Orders and at the direction of the COR. This may include diverting Level II Armed Protective Security Officers from their posts to meet the condition and summoning appropriate assistance as may be required. Level II Armed Protective Security Officers shall immediately make notifications as directed in the Post Orders.

2.9.2 Level II Armed Protective Security Officers shall immediately report all potentially hazardous conditions and items in need of repair, including inoperative lights, locks, security hardware, leaky faucets, toilet stoppages, broken or slippery floor surfaces, blocked emergency routes or exits, etc.

2.9.3 Level II Armed Protective Security Officers 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 in the facility or on the grounds.

2.9.4 Level II Armed Protective Security Officers 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, Level II Armed Protective Security Officers shall verbally report threatening circumstances and potentially threatening activities they observe to the COR, or the onsite FEMA Security Manages. Whenever possible, Level II Armed Protective Security Officers will 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 Level II Armed Protective Security Officers 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 public lawfully in facilities or on the grounds under the control of the Government.

2.10. ASSIGNMENT AND SIGN-IN

2.10.1. The Prime Contractor shall be responsible for scheduling all work and notifying Level II Armed Protective Security Officers of their work schedules in a manner consistent with effective Attachment 01 - Guard Task Order Form.

2.10.2. When requested by the CO or COR, the Contractor shall furnish a copy of the most current schedule of times, and Level II Armed Protective Security Officers by name that will be on post to the Government and provide a weekly schedule.

2.10.3 All Level II Armed Protective Security Officers must be in **Prime Contractor** 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. No mix matching uniforms or Prime/Subcontractors.

2.10.3.1 If a Subcontractor is utilized to perform Level II Armed Protective Services. The Subcontractor must have an agreement with the Prime Contractor. The Subcontractor is held to the same standards within the PWS and Agreement.

2.10.4 The Prime Contractor and subcontractor's employees shall sign in when reporting for work, and shall sign out when leaving, on Attachment 10 - GSA Form 139, Level II Armed Protective Security Officers Duty Register. Guards working overnight will sign out at 2400 and sign in at 0001 for billing purposes at the change of the calendar day. A copy of the 139's will be maintained by the contractor and submitted attached to the invoice.

2.10.4.1 Each successively lower line on Attachment 10 - GSA Form 139 must be completed in chronological order, without exception. Lines may not be left blank among signatures in any period. Each calendar day shall be a new Attachment 10 - GSA Form 139.

2.10.4.2 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 GSA 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.

- Level II Armed Protective Security Officer shall draw a single line through the entire line on which such mistakes appear.
- The Contractor must attach a detailed memorandum of explanation to each GSA 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.

2.10.4.3 The Contractor shall not remove the GSA 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 GSA Form 139s from the post, payment may not be made until the original forms are received by the COR.

2.10.5. Level II Armed Protective Service Officer who patrol between buildings will sign in and out at each facility visited. The Level II Armed Protective Service Officer will sign in and out at each post visited. Attachment 09 - Security Guard Post Assignment Record (Post Orders), specifically FEMA Security PSO Activity Log.

2.11. CONTRACT MODIFICATIONS:

The Contractor may be financially liable for accepting or implementing changes that affect the Contract (Attachment 01 Guard Task Order, Attachment 09 Post Orders) 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 PWS. The contractor will be tasked with specific sites and location, hours required, and duty responsibilities. The sites, hours and locations could change on a daily basis at the direction of FEMA OCSO Security personnel through the Contracting Officer and COR.

Contractor will have the capability of providing **20 Level II Armed Protective Security Officers** as employees at the time of signing of the Contract.

- Armed - Guard Level II (ESS) - To be invoiced against CLIN 0001

3.1. MINIMUM QUALIFICATIONS.

3.1.1. All Level II Armed Protective Security Officers and Armed Protective Security Supervisors performing under the resulting contract/orders must meet the following minimum qualifications:

- U.S. Citizenship
- Proficiency in English (written and spoken)
- High school diploma, GED certificate, college transcripts military records or POST

training completion

- Current or prior military and/or security experience
- Active Federal, State and Local Firearms permit(s) as applicable
- Have all state/local licenses, permits, registrations, or certifications as required to perform the duties and responsibilities of the position.
- State Security Officer Certification (as required)
- Local permits and renewals (as required)
- CPR, First Aid, and AED certification card.
- Firearm licenses and certifications required by state and local requirements.
- Current firearms training and qualification
- Current baton or OC certification
- Must be at least 21 years of age.
- Grooming Standards
 - Level II Armed Protective Security Officers are expected to be clean and properly groomed at all times. Your uniform must be clean, unwrinkled and properly fitting when you report for duty. Uniforms, insignia, accessories and equipment clean and in good repair. The uniforms are to be maintained and worn.
 - Level II Armed Protective Security Officers fingernails will be clean, trimmed (manicured), and not hinder the deployment of your assigned firearm. Nail polish must be worn if it is basic, or natural looking.
 - Level II Armed Protective Security Officers hair must be clean, neat and not interfere with the proper wearing of official headgear. Hair must be kept above shoulder length, maintained/secured in ponytail and not extend past the collar. Hair must not interfere with vision or be worn loose.
 - Level II Armed Protective Security Officers facial hair must be clean and manicured.
 - Level II Armed Protective Security Officers makeup may be worn, provided it is subdued and natural looking. While you are on duty, you may wear jewelry such as earrings (posts/studs), and must not wear dangling earrings, bracelets, body piercings, chains, buttons, or pendants.
 - Level II Armed Protective Security Officers tattoos must not have any lewd or offensive indelible marks.

3.1.2. Records of firearms qualifications. Prime Contractor must maintain records of their employees' successful completion of local and state firearms or other training requirements and possession of a current weapons permit, and upon request (Contracting Officer or Contracting Officer's Representative) produce the weapons/permits/certification(s) for immediate inspection at the work location/job site.

3.1.2.1 Use of Force Guideline or Policy. Contractor must provide a copy of their company Use of Force Guideline or Policy updated within 24 hours of the Contract.

3.1.3. Work experience requirement. Each Level II Armed Protective Security Officer 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 Level II Armed Protective Security Officers 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. The following are the essential job functions for uniformed employees working under the Contract:

- Physically detaining and escorting an individual with assistance.
- Work greater than 12-hour days and can work additional hours due to unexpected activity. *(Disclaimer may be approved by the COR in writing if requested.)*
- Work under occasional tension or pressure.
- Work alone while armed.
- Frequent and prolonged walking, standing, sitting, and stooping.
- Apply handcuffs.
- Use of handgun, make shoot/no-shoot decision with handgun, fire handgun.
- Occasional running or sprinting.
- Respond to life threatening or emergency.
- Climb while in pursuit or in an emergency situation (stairs, etc.).
- Pull oneself over an obstacle.
- Lift/carry/drag/pull/push heavy objects.
- Physically control crowds or by-standers.
- Pursue suspects on foot and subdue combative person after running in pursuit.
- Any other related duties within the PWS & attachments.

3.3. SUITABILITY

3.3.1. All Level II Armed Protective Security Officers may begin working Post when the following documents (Suitability Package Documents) are received by the COR:

- Attachment 11 - Contractor DHS Fitness Form 11000-25
- Attachment 12 - Optional Form 306, Declaration for Federal Employment (OF306)
- Attachment 13 - Lautenberg
- Attachment 14 -DHS Form 11000-6, Sensitive but Unclassified Non-Disclosure Agreement Amendment Statement
- Attachment 15 - DHS Form 11000-9

3.3.2. All Level II Armed Protective Security Officers will have their Suitability Package reviewed within 72 hours by FEMA Security Specialist and Security Managers. All errors will be returned to the Contractor for corrections. The Contractor has 72 hours to have it resolved/updated and returned to the identified FEMA COR. Failure to update/resolve and returned. The COR will notify the Contractor to remove the Level II Armed Protective Security Officer from Post.

3.3.3. All Level II Armed Protective Security Officer(s) will have their first and last name, Serial Number last four digits checked against Integrated Security Management System (ISMS).

3.3.3.1. If the name/Serial Number last four digits is returned as Entrance of Duty Date (EOD) Denied. They do not stand Post and not to be reran for suitability/fitness.

3.3.3.2. If the name/Serial Number last four digits is returned as non-compliant. The Level II Armed Protective Security Officers failed to answer two prior emails from a Personal Security Case Worker (*Level II Armed Protective Security Officers shall check SPAM/JUNK FOLDER*). The Level II Armed Protective Security Officers will not be allowed to stand Post. The Level II Armed Protective Security Officers is allowed to resubmit the Suitability Package Documents. But will not stand post until EOD Approved.

3.3.4. All Level II Armed Protective Security Officer(s) who have been EOD approved, worked for a prior company, or on another Contract, must submit Attachment 11 - Contractor DHS Fitness Form 11000-25 to be switched to the current Contract.

- Personal Security (PER SEC) may approve/disapprove submit Attachment 11 - Contractor DHS Fitness Form 11000-25 or request resubmittal of Suitability Package Documents (See 3.3.1).

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 Level Armed Protective Security Officers, whether armed or unarmed, rises to the level of Public Trust Moderate Risk.

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

3.4.3.1 A waiver is in place for up to 120 days due to the declared disaster, that supersedes 3.4.3., as long as the conditions of 3.3 Suitability are met.

3.4.4. Facility Access

3.4.4.1 The Contractor shall comply with FEMA Directive 121-1 "FEMA Personal Identity Verification Guidance," FEMA Directive 121-3 "Facility Access," and FEMA Manual 121-3-1 "FEMA Credentialing Access Manual," to arrange for contractor personnel's access to FEMA facilities, which includes, but is not limited to, arrangements to obtain the necessary identity badges for contractor personnel in accordance with Homeland Security Presidential Directive-12.

3.4.4.2 FEMA may deny facility access to any contractor personnel whom FEMA's Office of the Chief Security Officer has determined to be a potential security threat.

3.4.4.3 The Contractor shall notify the FEMA COR of all terminations/resignations within five

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

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

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

3.4.4.5 The Contractor or contractor personnel's failure to return all DHS or FEMA-issued identification cards and building passes upon expiration, upon the contractor personnel's removal from the contract, or upon demand by DHS or FEMA may subject the contractor personnel and the Contractor to civil and criminal liability. FEMA reserves the right to withhold the last invoice until DHS FEMA-issued identifications cards, building passes, and/or Report (See 3.4.4.3.) are received.

3.4.4.6 The Contractor shall maintain record of the fitness approval paperwork in the individual's local personnel folder or file.

3.4.4.7 The Contractor shall be solely responsible for any delay in the performance of this contract due to any failure by the Contractor's employees and subcontractors, if applicable, to provide accurate information on the background investigation forms submitted to FEMA for processing. If the background investigation package is incomplete, FEMA Personnel Security will return the incomplete package to the individual for correction. An incomplete background investigation package will not excuse the Contractor from meeting the contract requirements in a timely manner.

3.4.4.8 The Government will exercise full and complete control over granting, denying, withholding, or terminating fitness for contracted employees at any time. The granting of either a preliminary or final fitness determination shall not prevent, preclude, or bar the withdrawal or termination of any such fitness determination by the Government. If an individual has been arrested at any time after the initial fitness determination was granted, then it is incumbent upon the individual to immediately notify his or her supervisor of such an occurrence. If the supervisor or Contractor management becomes aware that an employee or subcontractor has been arrested at any time after the initial suitability was granted, the Contractor must notify the COR in writing within 12 hours of receiving that information.

3.4.4.9 If there is any disqualifying information that renders an individual unfit to perform his or her required duties as determined by the COR, then the individual shall be removed from duty.

3.4.4.10 The Contractor shall be able to provide up to **20**-Level II Armed Protective Security Officers, within 24 hours of the effective date of this Contract. The Contractor shall provide armed guard services for additional sites identified after the initial effective date within 24 to 48 hours after an LUA/Lease/MOU is signed.

3.4.4.11 The Contractor shall submit a minimum of **20** vetted Guard packets at the start of the Contract at no cost to the Government.

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. Otherwise, the Contractor shall provide a fully qualified replacement.

3.6. PROJECT MANAGER

The Contractor shall identify a Project Manager who shall be responsible for all Contractor work performed under this PWS. 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. Level II Armed Protective Security Officers are expected to always conduct themselves in an acceptable manner. While on post, Level II Armed Protective Security Officers will not engage in the following:

3.7.2.1. Engaging in any disallowed activities while standing post

3.7.2.2. Non-official fraternization with building occupants or visitors

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

3.7.2.4. Eating or using any tobacco product on post

3.7.2.5. Reading newspapers, books, magazines, etc. on post

3.7.2.6. Using, watching, or listening to non-official audio or video devices on post

3.7.2.7. Sleeping, dozing, or napping on post

3.7.2.8. Playing cards or other games on post

3.7.2.9. 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 an Level II Armed Protective Security Officers from a 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 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 generally inappropriate behavior 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 Contractor 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 Attachment 19 - 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 NDA 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 [OPSEC Awareness for Military Members, DOD Employees and Contractors](#)

Send the certificate of completion to the FEMA COR no later than 30 calendar days after 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 (Performance Work Statement, 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:

4.1.3.1. Contractors and Subcontractors who are working on this Contract shall receive the Unauthorized Disclosure of Classified or Unclassified Information training when the Contract is issued. Access to the training can be obtained at: <https://www.dhs.gov/dhs-security-and-training->

[requirements-contractors.](#)

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

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

4.2. PERIOD OF PERFORMANCE

The period of performance is base **3 Months, and 3 Options of 3 Months.**

4.3. PLACE OF PERFORMANCE

Although the specific site locations will vary, they will be within the State/Territory designated in the disaster declaration. Locations will be specified in Call Order or verbally until followed up with a written Call Order. The types of locations for which Level II Armed Protective Security Officers will be required include:

- Joint Field Offices and Annex
- Branch Offices
- Initial Operating Facilities
- Disaster Relief Centers
- Mobile Disaster Relief Centers
- Logistical Staging Areas
- Communications Centers
- Responder Base Camps
- Temporary Military Bases
- Urban Search and Rescue Staging and operational sites
- Temporary Group Sites
- Temporary Housing Centers
 - Commercial Parks
 - Group Sites
 - Private Sites
- Ships
- 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 Call Order or verbally until followed up with a written Call Order. Limitation on 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 a Contract that exceed maximum allowed hours of service as set by applicable federal, state, or local law.

4.5. TRAVEL: Travel will not be paid and is a part of the **Firm-Fixed-Price or Labor Hour Rate**.

In the event lodging is limited and FEMA has FEMA Responder Lodging, the Company may utilize lodging in Responder Lodging to house PSO's. Approval must be obtained from the Contracting Officer prior to the use of this lodging. If approval is made the Contracting Officer may adjust Lodging, Lodging Tax, and M&IE. The Contracting Officer will may adjust based on type of lodging and if meals are provided by the Responder Lodging program. See Attachment 19 - Security Equities in Standing Up Responder Lodging Locations During Disaster Operations.

4.6. POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than three (3) business days after the date of Call Order. 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 or via teleconference TBD.

4.7. PROJECT PLAN

The Contractor shall provide an updated 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 update the Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 30 days after the date of the Contract. 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 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 contact 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, Contractor Type (Prime/Subcontractor), all direct costs by line item, an assessment of technical progress, schedule status, weapon assignment by company, employee with serial number and 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 on **TBD** basis by phone or email.

4.10.2. The Project Manager shall also be available to meet personally with the COR on a **TBD** basis to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place at **TBD**.

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 or higher and Microsoft Office Applications). The following reports due:

- Daily Reports
- Weekly reports
- Monthly Reports
- Annual Reports
- Contract Clauses Requested Documents Checklist with suspense date will be provided.
- File Transition – Turn over documents End of Contract/Contract
- See Attachment 20 – Section F – Deliverable Schedule
- See Attachment 22 – 11.5 Spreadsheet

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.

4.12.1.1. Phase-In of Contract/Contract and Continuity of Services

4.12.1.2. 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, if there is no interference with the 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.

4.12.1.3. The Contractor shall provide a transition plan within fourteen (14) working days after the Contract has been awarded. 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 Call Order 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 (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/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 PWS:

- 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)
- Performance Work Statement (PWS)
- 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 has provided the references cited in PWS 1.4 at attachments. See Section J – List of attachments.

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
- Safety Strap: Left/Right as Required
- Double Magazine Case or Speed Loader Case Compatible with Specified
- Weapon and Ammunition in accordance with 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
- Level II Ballistic Resistant vest
- Held Wand/Magnetometer
 - 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)
 - Fencing (when deemed necessary)

** 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.

*** All outer wear must be issued by the company, matching colors, and company insignia.

NOTE: Each subcontractor must wear the prime contractor’s uniform and patches, unless approved by the COR. Each site must have uniform integrity (matching).

7.2. FIREARMS AND AMMUNITION

7.2.1. All Level II Armed Protective Security Officers will carry only Contractor-authorized duty weapon consisting of semiautomatic weapon of .9mm or .40 caliber.

7.2.2. Common factory law enforcement ammunition shall be used, no reloads.

7.2.3. Contractors shall provide firearms and ammunition to the Level II Armed Protective Security Officers and Contract Security

7.2.4. Guards shall carry three ammunition magazines. Each magazine carried will be full of ammunition. Two magazines will be spares and carried on the duty belt in a holder designed for that purpose. One magazine will be inserted in the handgun. The weapon will have a round in the chamber. Level II Armed Protective Security Officers shall engage all safety features on the weapon and shall always follow all appropriate safety procedures.

7.2.5. No personal weapons are authorized in the performance of this contract.

7.2.6. No weapons that have been modified from the original manufacturer's specifications are authorized in the performance of this contract.

7.2.7. All safety features on all weapons must be operational and engaged.

7.2.8. All ammunition will be Contractor-issued and will also meet manufacturer's specification.

7.2.9. If the Contractor employs state or local law enforcement officers (LEOs), they will wear the uniform of the Contractor. If approved by the Program Office OCSO, FOD for LEOs to carry state or local departmental weapons on this contract.

7.2.9.1. If the LEO is utilizing a state or local agency weapon. An Agency representative must sign off and provide the names and weapon serial numbers giving consent for the LEO to carry the agency owned firearm on the contract.

7.2.10. Appropriate and ample supplies of firearms maintenance equipment (cleaning solvents, lubricating oil, rods, brushes and patches, and other normal maintenance tools) shall be provided by the Contractor and at the Contractor's expense.

7.2.11. Each individual Level II Armed Protective Security Officers will utilize only his own Contractor assigned weapon and ammunition, with one weapon being assigned to only one person. There will be no sharing of weapons or assigning weapons to a post and not a person. The Contractor's employees shall inspect their assigned firearms at the commencement of each tour of duty. Each firearm shall be cleaned and oiled regularly to ensure optimum operating condition. Firearms shall always be handled in a safe and prudent manner.

7.2.12. The Contractor must be able to always account for all firearms and ammunition.

7.2.13. The Contractor shall provide a list of serial numbers of all firearms that will be carried during this Contract. The list shall be kept current; the Contractor must document and forward any changes to the COR when a change occurs.

7.2.14. In the event that a firearm is discharged, lost or stolen, the Contractor shall notify the FEMA Security Manager and COR immediately and shall relay all the particulars known regarding the discharge, loss or theft of the weapon. Additionally, the Contractor shall provide a detailed written report to the COR within 4 hours of the incident, including the date and time of the incident. The Contractor shall also notify the COR of the serial number for the replacement weapon.

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. Level II Armed Protective Security Officers 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. Level II Armed Protective Security Officers 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 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 PWS. Coordinate with COR if dates are not entered.

- See Section J, List of Attachments.
 - Attachment 20 – Section F – Deliverable Schedule

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

10.1.2. Performing surveillance of the Contractor employees while they are on duty

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

10.1.4. Ensuring compliance with Contract(s), Guard Task Order(s), and Security Guard Post Assignment Record (Post Orders) requirements as the Level II Armed Protective Security Officers duties and behavior are concerned.

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

10.1.6. 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.

10.4 PERFORMANCE REQUIREMENTS SUMMARY (PRS)

The PRS establishes key elements of Contractor performance that represent "mission essential" service requirements, which are identified in the table below in the "Service Output" column. The "Performance Objective" column represents the standard against which Contractor performance will be measured in relation to accomplishment of the corresponding service output. The performance objective or "standard" describes the minimum acceptable level of service by the Contractor for satisfactory performance. The "Acceptable Quality Level (AQL)" column displays the maximum allowable deviation from the performance objective, which, if exceeded, evokes the negative incentive specified in the table below.

- See Attachment 21 - Performance Requirement Summary (PRS)

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

11.1. Prior to the Contract start date, and except where precluded by local law or ordinance, the Contractor shall make and complete all arrangements with the appropriate officials in the city, county/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 Contract Level II Armed Protective Security Officers and Security Supervisor. Contract Level II Armed Protective Security Officers 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 an Level II Armed Protective Security Officers to carry a valid firearm certificate or permit while on duty shall result in the Contract Level II Armed Protective Security Officers 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 PWS. 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 e-mail a **spreadsheet** showing employee compliance in accordance with contract/Contract policy. 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 so as to ensure that all legal requirements have been fulfilled prior to the commencement of any and all work under the Contract.

- See Attachment 22 - 11.5 Spreadsheet

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 and permits 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.

Important Note: 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/Contract employee's files at any time during the course of the Contract. The Contractor shall maintain all personnel files for a minimum of six (6) years after 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 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/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 its 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 PWS. 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, e- mailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the PWS. 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.
11. The Contractor shall CC fema-ocso-contracts@fema.dhs.gov on all e-mails.
12. The Contractor shall use the following subject E-mail on the subject line: DR-4933-IN – Contract # - Subject
 - **Example of Subject Line:** DR-4673-FL - 70FBR426F00000001 – Subject
13. The Contractor shall utilize the following naming conventions in documentation:

Contract #	Contract #	Subject	Start Date	Through	End Date	Location if applicable
DR-####-##	Insert #	139	YYYYMMDD	-	YYYYMMDD	Name
DR-####-##	Insert #	Invoice and Invoice #	YYYYMMDD	-	YYYYMMDD	
DR-####-##	Insert #	Progress Report	YYYYMMDD	-	YYYYMMDD	
DR-####-##	Insert #	Schedule	YYYYMMDD	-	YYYYMMDD	

Contract #	Contract #	Subject	Subject
DR-####-##	Insert #	Deliverable	Kickoff Meeting Excel
DR-####-##	Insert #	Deliverable	Active License
DR-####-##	Insert #	Deliverable	Business Continuity Plan
DR-####-##	Insert #	Deliverable	Draft Project Plan
DR-####-##	Insert #	Deliverable	Final Project Plan
DR-####-##	Insert #	Deliverable	Insurance
DR-####-##	Insert #	Deliverable	State Registration
DR-####-##	Insert #	Deliverable	Transition Plan
DR-####-##	Insert #	Deliverable	Use of Force
DR-####-##	Insert #	Deliverable	Weapons Roster

Contract #	Contract #	Subject	PSO Name	Document	Date
DR-####-##	Insert #	Deliverable	Name	Guard License	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	Firearms License	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	CPR	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	First Aid	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	AED Certification	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	Firearms Qualification	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	Baton Certification	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	OC Certification	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	TBD IAW PWS	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	TBD IAW PWS	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	TBD IAW PWS	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	TBD IAW PWS	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	TBD IAW PWS	YYYYMMDD
DR-####-##	Insert #	Deliverable	Name	TBD IAW PWS	YYYYMMDD

DR-####-##	Insert #	Deliverable	Name	TBD IAW PWS	YYYYMMDD
------------	----------	-------------	------	-------------	----------

14. **508 INFORMATION TECHNOLOGY CLAUSE**

[Test for Accessibility | Section508.gov](#)

<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 PWS.

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.

INFORMATION SHARING

To accomplish the tasks outlined in this contract, FEMA will provide the contractor with access to limited PII consistent with security procedures in the Electronic Security System (ESS), including Personal Identity Verification (PIV) card information and facility visitor names. The contractor will not have direct access to ESS.

The information sharing outlined in this contract is authorized by the following System of Records Notice(s) and Routine Use(s):

- [DHS/ALL-023 Department of Homeland Security Personnel Security Management](#), October 13, 2020, 85 FR 64511, Routine Use H.
- [DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management](#), February 3, 2010, 75 FR 5609, Routine Use F.
- [DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records](#), June 14, 2017, 82 FR 27274, Routine Use F.
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, June 25, 2009, 74 FR 30301, Routine Use F.

The information sharing outlined in this contract is authorized by the following Privacy Impact Assessments:

- DHS/FEMA/PIA-051 FEMA Physical Access Control Systems (PACS)

Need to Know

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

Prohibition on Computer Matching

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

Return or Destruction of Data when no longer needed

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.

Clauses

- 1) HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information (July 2023)
- 2) Special Clause Information Technology Security Awareness Training
- 3) HSAR 3052.204-71 Contractor Employee Access
- 4) HSAR 3052.204-73 HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents
- 5) 52.204-9 Personal Identity Verification Of Contractor Personnel (JAN 2011)
- 6) 52.224-1 Privacy Act Notification (APR 1984)
- 7) FAR 52.224-3 Privacy Training – Alternate I (see FAR Class Deviation 17-03, Revision 1)

HSAR 3052.240-72 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (HSAR DEVIATION 25-12) (Effective November 3, 2025)

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

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

- (1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, “Chemical Facility Anti-Terrorism Standards,” and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual “Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information” dated September 2008);
- (2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII’s implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;
- (3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, “Protection of Sensitive Security Information,” 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 designee), including Department of Homeland Security MD 11056.1, “Sensitive Security Information (SSI)” and, within the Transportation Security Administration, TSA MD 2810.1, “SSI Program”;
- (4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;
- (5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;
- (6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;
- (7) Information Systems Vulnerability Information (ISVI) means:
 - (i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

- (A) Truncated SSN (such as last 4 digits);
- (B) Date of birth (month, day, and year);
- (C) Citizenship or immigration status;
- (D) Ethnic or religious affiliation;
- (E) Sexual orientation;
- (F) Criminal history;
- (G) Medical information; and
- (H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is

critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

- (1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
- (2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

- (1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- (2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- (3) Availability, which means ensuring timely and reliable access to and use of information.

Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) Handling of Controlled Unclassified Information.

- (1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>.
- (2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.
- (3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.
- (4) Any government data provided, developed, or obtained under the contract, or otherwise under the

control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) *Incident Reporting Requirements.*

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, 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) Unique Entity Identifier (UEI);
- (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, and email);
- (v) Contracting Officer POC (address, telephone, and 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 CUI resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the government PII or SPII contained within the system; and
- (xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

- (1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting 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 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;
 - (iv) Data analyses and processing; and
 - (v) Revocation of the Authority to Operate (ATO), if applicable.
- (4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.
- (5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(e) *Certificate of Sanitization of Government and Government-Activity-Related Files and Information.* Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, *Guidelines for Media Sanitization*. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization*, Appendix G.

(f) *Other Reporting Requirements.* Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) *Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

16. **SPECIAL CLAUSE INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)**

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

(b) *Security Training Requirements.*

- (1) 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 31 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 <https://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 31 of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.
- (2) 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 <https://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.

HSAR 3052.240-73 NOTIFICATION AND CREDIT MONITORING REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION INCIDENTS (HSAR DEVIATION 25-12) (Effective November 3, 2025)

(a) *Definitions.* Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual’s identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an

individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

- (i) Truncated SSN (such as last 4 digits);
- (ii) Date of birth (month, day, and year);
- (iii) Citizenship or immigration status;
- (iv) Ethnic or religious affiliation;
- (v) Sexual orientation;
- (vi) Criminal history;
- (vii) Medical information; and
- (viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) PII and SPII Notification Requirements.

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction 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 or 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, mitigate the incident, and protect against any future incidents; and
- (vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements.* The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the 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.

(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 Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
- (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

Privacy Training – Alternate I (Deviation)

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

- (b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who-
 - (1) Have access to a system of records;
 - (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
 - (3) Design, develop, maintain, or operate a system of records (see also FAR subpart [24.3](#) and [39.105](#)).
- (c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract.
 - (1) "Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover-
 - (i) The provisions of the Privacy Act of 1974 ([5 U.S.C. 552a](#)), including penalties for violations of the Act;
 - (ii) The appropriate handling and safeguarding of personally identifiable information;
 - (iii) The authorized and official use of a system of records or any other personally identifiable information;
 - (iv) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access personally identifiable information;
 - (v) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and
 - (vi) The procedures to be followed in the event of a suspected or confirmed breach of a system of records or the unauthorized disclosure, access, handling, or use of personally identifiable information (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).
 - (2) Completion of an agency-developed or agency-conducted training course shall be deemed to satisfy these elements.
- (d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
- (e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.
- (f) The substance of this clause, including this paragraph (f), shall be included in all

subcontracts under this contract, when subcontractor employees will-

- (1) Have access to a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or
- (3) Design, develop, maintain, or operate a system of records.

HSAR 3052.240-71 CONTRACTOR EMPLOYEE ACCESS (JULY 2023) (HSAR DEVIATION 25-12) (Effective November 3, 2025)

(a) *Controlled Unclassified Information (CUI)* is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

- (1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, “Chemical Facility Anti-Terrorism Standards,” and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual “Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information” dated September 2008);
- (2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII’s implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;
- (3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, “Protection of Sensitive Security Information,” 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 designee), including Department of Homeland Security MD 11056.1, “Sensitive Security Information (SSI)” and, within the Transportation Security Administration, TSA MD 2810.1, “SSI Program”;
- (4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;
- (5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;
- (6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;
- (7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

- (A) Truncated SSN (such as last 4 digits);
- (B) Date of birth (month, day, and year);
- (C) Citizenship or immigration status;
- (D) Ethnic or religious affiliation;
- (E) Sexual orientation;
- (F) Criminal history;
- (G) Medical information; and

(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

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

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

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

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

HSAR 3052.240-71 CONTRACTOR EMPLOYEE ACCESS ALT II (HSAR DEVIATION 25-12) (Effective November 3, 2025)

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

(End of clause)

PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011)

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

(b) The Contractor shall account for all forms of Government-provided identification issued to the Contractor employees in connection with performance under this contract. The Contractor shall return such identification to the issuing agency at the earliest of any of the following, unless otherwise determined by the Government:

- (1) When no longer needed for contract performance.
- (2) Upon completion of the Contractor employee's employment.
- (3) Upon contract completion or termination.

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

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

SECURITY LANGUAGE – Unclassified only

All personnel require access to unclassified information only. Contractors must ensure contractor employees receive a favorably background investigation prior to entry on duty (EOD). All individuals will be U.S. citizens or lawful permanent residents. The contractor shall follow the standards established within DHS and FEMA policy.

OPSEC Training:

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

Access to the briefing can be obtained at [OPSEC Awareness for Military Members, DOD Employees and Contractors](#)

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

Insider Threat Training:

Insider Threat training for Contractors can be found at: [Insider Threat Awareness](#)

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

Background Investigations

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

Low Risk without Information System Access

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

Low Risk with Information System Access

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

Moderate Risk

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

High Risk

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

Background Investigation Process

To initiate the request to process contractor personnel, the Contractor shall provide the FEMA Contracting Officer's Representative (COR) with all required information and comply with all necessary instructions to complete Section II of the FEMA Form 121-3-1-6, "Contract Fitness/Security Screening Request." The FEMA COR shall ensure that all other applicable sections of the FEMA Form 121-3-1-6 are complete prior to submitting the form to FEMA PSD for processing. The Contractor shall also provide the FEMA COR with completed OF 306, "Declaration for Federal Employment," forms for all contractor personnel.

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

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

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

For those contractor personnel who do not have an acceptable, prior, favorable adjudication or who otherwise require reinvestigation, FEMA PSD will issue an electronic notification via email directly to the contractor applicant/personnel that contains the following documents, which are incorporated into this contract by reference, along with a link to the National Background Investigation Services (NBIS) e-Application (eAPP) online system and instructions for submitting the necessary information:

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

FEMA PSD will only accept complete packages consisting of all of the above document and Standard Form 85P, which must be completed electronically through the National Background Investigation Services (NBIS) e-Application (eAPP) online system. The Contractor is responsible for ensuring that all contractor personnel timely and properly submit all required background information.

Once contractor personnel have properly submitted the complete package of all required background information, FEMA's Personnel Security Division, at its sole discretion, may grant contractor personnel temporary eligibility to perform work under this contract prior to completion of the full background investigation if the Personnel Security Division's initial review of the contractor personnel's background information reveals no issues of concern. In such cases, FEMA's Personnel Security Division will provide notice of such temporary eligibility to the COR who will then notify the Prime Contractor, at which time the identified contractor personnel will be temporarily eligible to begin work under this contract. Neither the Prime Contractor nor the contractor personnel has any right to such a grant of temporary eligibility. The grant of such temporary eligibility shall not be considered as assurance that the contractor personnel will remain eligible to perform work under this contract upon completion of and final adjudication of the full background investigation.

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

Continued Eligibility and Reinvestigation

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

Exclusion by Contracting Officer

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

Foreign Travel and Government-Issued Equipment

Per DHS and FEMA IT policy, FEMA employees and contractors are not authorized to take government-issued equipment, including cell phones, computers, or tablets such as iPads, outside of the United States regardless of the reason for travel. If government-issued equipment is required for official foreign travel, FEMA government employees may request having their equipment configured for international travel or a temporary loaner device by completing FEMA Form 122-1-1-1, through the [ServiceNow](#) portal. FEMA contractors must contact their contracting officer's representative (COR) for further guidance.

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

Facility Access

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

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

Contractor personnel shall not receive a FAC until they have submitted a SF 87, “Fingerprint Card,” and an OF306, Declaration for Federal Employment, and receive approval from FEMA PSD. Contractor personnel using a FAC for access to FEMA facilities must be escorted in Critical Infrastructure areas (i.e., server rooms, weapons rooms, mechanical rooms, etc.) at all times.

FEMA may deny facility access to any contractor personnel whom FEMA’s Office of the Chief Security Officer has determined to be a potential security threat.

Separation of Contract

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

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

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

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