DIRECT LEASE PROGRAM
STATEMENT OF WORK (SOW)
DR-4781-TX- DR-4798-TX
UNITED STATES DEPARTMENT OF HOMELAND SECURITY
FEDERAL EMEGENCY MANAGEMENT AGENCY (FEMA)

PURPOSE

The Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA) specifies certain requirements for Direct Lease Vendor/Property Management Companies (Vendor/PMC) and/or Property Owners (PO). The FEMA Direct Lease is a housing assistance program to lease turnkey, existing rental units for the purpose of providing temporary housing to eligible applicants who are displaced by the Severe Storms and Flooding and Hurricane Beryl.

SCOPE

The contractor shall identify and provide residential properties located no more than 60 minutes from the damaged dwellings in specified Texas counties (Jasper, Liberty, Polk, San Jacinto, Trinity, and Tyler) to support eligible disaster applicants.

The contractor shall locate and curate a list of residential properties that fulfill the following criteria:

- Must be located within a 30 to 60-minute travel distance from the specified damaged dwelling.
- Eligible properties include existing residential properties advertised for lease (e.g., corporate apartments, vacation rentals, second homes); vacant residential properties available for sale or lease (single-family homes and multiple occupancy units); and bank-owned properties (e.g., foreclosures).
- **Properties must be turnkey ready; comply with federal, state, and local occupancy standards; provide complete and independent living facilities for one or more persons, including permanent provisions for living, sleeping, cooking, and sanitation. All utilities, appliances, and any furnishings provided must be safe and functional.**
- Also eligible are any other type of residential property that meets HUD criteria for Direct Lease properties.

Contractor Qualifications. Experience in property management, leasing, or real estate services within the target counties. Knowledge of FEMA regulations and disaster recovery processes. Strong communication skills and ability to work effectively with diverse stakeholders. By adhering to this Statement of Work, the contractor will effectively serve the needs of disaster applicants in Texas while meeting FEMA's requirements for temporary housing solutions.

DELIVERABLES

The contractor will identify and create a list of eligible properties with details such as location, type, rental/sale price, and availability status. The contractor will then provide regular updates to FEMA that summarize progress and challenges. The process should conform to the requirements below.

Compliance with FEMA Standards: Ensure that all identified properties comply with the standards outlined by FEMA for Direct Lease properties and any additional requirements specified in this Statement of Work.

Hardship Consideration: Ensure that the identified properties do not impose undue hardship on eligible disaster applicants, considering several factors such as accessibility, property conditions, affordability, safety features, wrap-around services, and proximity to basic amenities.

Prioritize Accessibility. Vendor/PMC shall seek out properties that include accessibility features or that can easily be modified to meet accessible requirements and are in proximity to accessible public transportation as well as wrap-around services, such as schools, emergency services, hospitals, pharmacies, etc.

Daily Progress Reporting: The vendor/project management company (PMC) shall provide FEMA with regular daily progress reports on property inventory. See Quality Assurance Surveillance Plan. (QASP)

Reports should include details on the number of properties found, property types, locations, availability, and any challenges encountered during the property acquisition process.

Communication and Coordination. The PMC shall maintain consistent communication with FEMA representatives and eligible disaster applicants to facilitate property viewings, lease agreements, and any necessary support services related to the leasing process.

Timeline. The PMC shall establish a timeline for property identification, reporting, and lease facilitation, ensuring prompt delivery of services to disaster applicants.

DETERMINATION

Vendor/PMC and FEMA shall evaluate each property to ensure the property is *safe, secure, sanitary*, and *functional*.

- *Safe* means no hazards or threats to occupants are present.
- *Sanitary* means free of all health hazards.
- *Functional* means an item or home is capable of being used for its intended purpose.
- *Secure* means free from danger or harm.

Acceptance Criteria. Suitable residential properties are identified successfully per all requirements; are in compliance with all FEMA/HUD regulations and standards; and have gotten positive feedback from eligible disaster applicants regarding the suitability and accessibility of provided properties.

Final Report upon Project Completion. A final report shall include overall findings, lessons learned, and any recommendations for improving future property identification efforts.

ADDITIONAL RESPONSIBILITIES OF VENDOR/PMC

Determining Cost. The monthly cost per unit may not exceed the amounts established in *Figure 1* below, unless an increase is approved by the Contracting Officer (CO).

Security deposit. The Government will establish a contract line item for one-month security deposit not-to-exceed one month rent. As a cost-reimbursable contract line item, the security deposit will not be disbursed at the signing of the contract. It will be held by the government in the event any damage (other than normal wear and tear) occurs and will be invoiced based on the actual cost of damage verified between the Government and the Vendor/PMC. All damage above the cost of monthly rent shall be the responsibility of the contractor and /or applicant upon confirmation of the cause of damage.

Security Deposit must be approved by Contracting Officer (CO) prior to submission of invoice. Vendor/PMC must submit a request for damage/security deposit within 30 days of move-out inspection (MOI). Documentation including repair costs and time-stamped photo documentation must be submitted with request. See attachment #4 "Direct Lease Contract Terms and Conditions" for additional information.

Waiver of application and background-check fees associated with the process of screening applicants. Vendor will inform property management company or property owners that credit checks will be waived in their entirety for all applicants occupying FEMA units.

Background checks will be processed within 24 hours after the applicant submits all pertinent information. Vendors shall provide FEMA with a daily status update on Background Checks (BGC) for each unit to be submitted by 9 a.m. Each morning. Vendor/PMC shall notify FEMA within one day if an applicant is being denied placement due to adverse information in their background check.

Tracking Spreadsheet. Vendor/PMC. Shall implement and update a tracking spreadsheet for approved properties throughout the Direct Lease process. The tracking system must be approved by the Contracting Officer's Representative (COR) prior to implementation. An example is provided at Attachment 2, Direct Lease Property Tracking Sheet.

Figure 1- Maximum Monthly Rent FY2025 Fair Market Rent Documentation **FMR**

County/Parish	1 BED	2 BEDS	3 BEDS	4 BEDS
Jasper County	$986	$1,167	$1,443	$1,548
Liberty County	$1,476	$1,763	$2,316	$2,879
Polk County	$987	$1,217	$1,465	$1,781
San Jacinto County	$1,240	$1,367	$1,698	$1,959
Trinity County	$973	$1,182	$1,420	$1,903
Tyler County	$1,281	$1,567	$2,054	$2,322

Property Inspections. Vendor/PMC and FEMA shall inspect each property to ensure compliance with Federal, State, and Local occupancy standards prior to executing lease agreements with housing applicants. Each inspection will also verify property owner's ability to provide all property management and building maintenance services. The property should be fully functional with all utilities working, and furniture assembled.

All properties managed by the Vendor/Property Management Company (PMC) are subject to inspection by FEMA and other applicable government agencies. The Vendor/PMC is required to actively participate in inspections by responding promptly to all requests for information and addressing any findings from regulatory agencies.

The Vendor/PMC must permit FEMA, or any entity or organization approved by FEMA, to conduct inspections of rental units as necessary. The inspections ensure that the services provided and the conditions of housing meet FEMA's standards and requirements.

HUD Inspection Form. All Vendors are required to submit the completed and signed HUD inspection form to FEMA for review prior to the scheduled walkthrough inspection. This form ensures that all necessary documentation is in order and facilitates a smooth inspection process.

The HUD inspection is considered complete when all functional areas of the unit are properly furnished and meet required standards, and each area is equipped with the necessary items and fixtures to function as intended.

Following the inspections, FEMA will share the findings with the Vendor/PMC, including the results from the HUD inspection form. (See Attachment 3.)

PLACING RESIDENTS IN A DIRECT HOUSING UNIT

Contacting Applicants. FEMA will identify eligible applicants for the Direct Lease program and provide the Vendor/PMC with contact information, including the applicant's name, co-applicant's name (if applicable), damaged dwelling address, mailing address, phone number(s), and email address.

Matching Applicants. Once suitable units are available, FEMA contacts applicants within one day to coordinate with them to match them with a Direct Lease unit that best fits their needs. FEMA also informs applicants of the next steps towards their placement in a Direct Lease Unit, such as having a background check for properties that require it.

Executing Lease Agreements. The Vendor/PMC shall execute lease agreements with FEMA through completion of *Attachment 4* of this document, the *Direct Lease Contract Terms and Conditions*.

Moving of Applicants. Vendor/PMC and FEMA will share responsibility for the move-in process of applicants into Direct Lease units. Vendor/PMC and FEMA shall conduct a walkthrough of the temporary housing unit with the applicant and ensure all the necessary paperwork is completed prior to completing a move-in. Within three (3) business days of completion, Vendor/PMC shall provide the COR with the following documents:

- A copy of the inspection record confirming the property complies with Federal, State, and local occupancy standards.
- Direct Lease Property Inspection Checklist (HUD) identified in (Attachment 3)
- The Direct Lease Contract Terms and Conditions (*Attachment 4*) completed in executing the lease agreement, specifying the monthly rental rate.
- A copy of the Direct Lease Occupant Lease Agreement (*Attachment 5*)
- A copy of the Temporary Housing Agreement (*Attachment 6*).

Lease Agreement Payments. FEMA shall make rental payments to Vendor/PMC in accordance with the terms and conditions of the fully executed FEMA Contract (contract between FEMA and Vendor/PMC) for each property that is awarded under the contract.

Terminating Lease Agreements.

- If a property must be terminated because it fails inspections twice that property will be terminated by default, because the vendor failed to provide a Turnkey property.
- FEMA will oversee the termination of assistance for applicants covered by FEMA Revocable License Agreement.
- Vendor/PMC shall be responsible for eviction of applicants whose assistance has been terminated by FEMA.
- FEMA may terminate the lease for the housing unit by providing Vendor/PMC with a written sixty (60) calendar day Termination Notice.

Utilities. FEMA is not responsible for utilities unless utilities are included in the monthly rental fee and do not exceed the established monthly rental rates.

Access and Functional Needs. A Vendor/PMC is allowed, at FEMA 's expense, to make reasonable modifications or improvements to the property to provide a reasonable accommodation for an eligible applicant with a disability or other access or functional needs. All modifications or improvements will be coordinated with the COR for FEMA approval prior to execution or incurring costs. All costs above $3,000 must be approved by the Contracting Officer.

Early Termination Fees. To be eligible for an Early Termination Fee, the Vendor/PMC must submit a copy of the lease between the Vendor/PMC and the Property Owner/Manager, to include the actual charges associated with the termination from the date of the cancellation. Early termination fees take effect when FEMA has provided the contractor with a sixty (60) calendar day Termination Notice. The early termination fee will be two (2) month's rent.

When an applicant is no longer eligible for Direct Housing Assistance and cannot remain in the leased unit, FEMA will notify the Vendor in writing, confirming that applicant has been notified of the termination and the effective date that the applicant must vacate the unit, removing all personal items and returning all keys to the Vendor.

If the applicant does not vacate the unit, the property owner is empowered to take the necessary steps to reclaim the unit using all legal action, including eviction.

When a Contractor initiates an early termination, they must give FEMA CO/COR a sixty (60) day notice with explanation. No early termination fee will apply.

MOVING THE APPLICANT OUT

The process is outlined below:

FEMA	Taskforce Lead notifies the COR and the CO when the unit is no longer needed, to terminate contract of the unit.
FEMA	COR notifies property management company or property owner that the occupant is moving out. (There is a standard template for the this)
FEMA/Vendor	Move Out Inspection is completed
Vendor	Vendor/PMC reports any damages to the Contracting Officer and COR within fourteen (14) days.
Vendor	In additional 14 days is allowed to submit the total costs to the Contracting Officer or COR.
FEMA	Complete FEMA Form FF-145-FY-21-100 with contract number, specific termination CLIN, Unit number, Address, and cost.
FEMA	Housing Unit Group Supervisor (HUGS) submits. FEMA Form FF-145- FY-21-100 to the Ordering Unit for routing to Contracting. Officer to process termination of unit by Contract Modification. (completed and signed by all parties to COR)
FEMA	CO is the only one who can issue a modification for termination of a unit. Once the modification is awarded and sent to Vendor/PMC, COR sends notice to property management company or property owner to return unit to their control as specified in the contract. If unit is no longer needed, Vendor/PMC will remove the unit from existing inventory.

Damage to Property. If there is damage to the property or rental furniture (if applicable), FEMA's security deposit may be used to cover the cost of any damage beyond normal wear and tear.

If property has been damaged, the Vendor/PMC reports damage to the Contracting Officer or COR within 14 days of the move-out inspection. An additional 14 days is allowed to submit the total cost to the Contracting Officer or COR.

LEGAL SECTION

QUALITY ASSURANCE/QUALITY CONTROL PROVISIONS

Vendor/PMC shall adhere to all quality assurance/quality control provisions outlined in the Quality Assurance Surveillance Plan.

Deliverables

(See Attachment 1 appendix1).

PLACE OF PERFORMANCE
Within 30 to 60 miles of disaster impacted counties. Jasper, Liberty, Polk, San Jacinto, Trinity, and Tyler in the State of Texas.

PERIOD OF PERFORMANCE
The period of performance (PoP):
Base POP: 12 months from contract award Option 1: 6 months
GOVERNMENT POINTS OF CONTACT:
CONTRACTING OFFICERS
[redacted]

CONTRACTING OFFICER REPRESENTATIVE(S):
[redacted]

PROGRAM MANAGER
[redacted]

Information Sharing

To accomplish the tasks outlined in this contract, FEMA will share with the contractor the following **PII/SPII** data elements:

Name
Street Number
City
Zip code.

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

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS) November 27, 2012, 77 FR 70792; Routine Use F.
- DHS/ALL-014 Department of Homeland Security Personnel Contact Information, March 16, 2018, 83 FR 11780; Routine Use F.
- OPM/GOVT-1 General Personnel Records, December **11,** 2012, 77 FR 73694, as modified by 80 FR 74815: Routine Use JJ.

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

- DHS/FEMA/PIA-006 DHS General Contact Lists.

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.

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

SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)

(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:

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);

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.

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"

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 FusionCenter Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015.

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.

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.

Information Systems Vulnerability Information (ISVI) means:

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 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.

(1) 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.

(2) 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.

(3) 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.

(4) 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.

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;

Ethnic or religious affiliation;

D. Sexual orientation;
E. Criminal history;
F. Medical information; and
G. System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

i. 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 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-trainingrequirements-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-trainingrequirements-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-validationprogram/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.*

All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.

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

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

Inspections;

Investigations;

Forensic reviews;

Data analyses and processing; and

Revocation of the Authority to Operate (ATO), if applicable.

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.

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.

(e) *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.

(f) *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.

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

(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

SECURITY LANGUAGE

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

Unauthorized Disclosure of Classified or Unclassified Information:

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

Access to the training can be obtained at: Unauthorized Disclosure of Classified Information and Controlled Unclassified Information (usalearning.gov)

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

OPSEC Training:

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

Access to the briefing can be obtained at OPSEC Awareness for Military Members, DOD Employees and Contractors (usalearning.gov)

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 (usalearning.gov)

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

FEMA

annually thereafter. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

For Official Use Only (FOUO) Information:

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

The contractor will:

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

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

Foreign Travel and Government-Issued Equipment:

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

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

Background Investigations:

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

federal position, applying the same standard for evaluating the associated potential for impact on the integrity and efficiency of federal service.

Low Risk without Information System Access:

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

Low Risk with Information System Access:

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

Moderate Risk:

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

High Risk:

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

Background Investigation Process:

To initiate the request to process contractor personnel, the Contractor shall provide the FEMA Contracting Officer's Representative (COR) with all required information and comply with all necessary instructions to complete Section II of the FEMA Form 11000-25, "Contract Fitness/Security Screening Request." The FEMA COR shall ensure that all other applicable sections of the FEMA Form 11000-25 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 contactor personnel will remain eligible to perform work under this contract upon completion of and final adjudication of the full background investigation.

Upon favorable adjudication of the full background investigation, FEMA's Personnel Security Division will update the contractor personnel's security file and take no further action. In any instance where the final adjudication results in

an unfavorable determination FEMA's Personnel Security Division will notify the contractor personnel directly, in writing, of the decision and will provide the COR with the name(s) of the contractor personnel whose adjudication was unfavorable. The COR will then forward that information to the Contractor. Contractor personnel who receive an unfavorable adjudication shall be ineligible to perform work under this contract. Unfavorable adjudications are final and not subject to review or appeal.

Continued Eligibility and Reinvestigation:

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

Exclusion by Contracting Officer:

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

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.

of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

PRIVACY TRAINING REQUIREMENTS

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

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

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 infonnational 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

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.

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 ofInformation 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.

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.

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.

The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the SOW. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or

maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to FEMA control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the SOW. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

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.

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

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.

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.

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.

3052.204-73 NOTIFICATION AND CREDIT MONITORING REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION INCIDENTS (JULY 2023)

(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 hann 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)