

## STATEMENT OF WORK FOR DIRECT LEASE DR-4724-HI

### PURPOSE

The Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) has a requirement for Direct Lease under the Presidentially declared major disaster DR-4724-HI for the State of Hawaii as a result of wildfires. Direct Lease is a form of direct temporary housing assistance where FEMA may enter into lease agreements with owners of existing residential property not typically available to the general public (e.g., corporate apartments, vacation rentals, and second homes) and make them available directly to eligible applicants for use as temporary housing. FEMA is using property management companies/managers (Contractor) to fulfill the Direct Lease requirements.

### SCOPE:

The Contractor shall locate, acquire, and manage an inventory of potential properties in Maui County, Hawaii. FEMA reserves the right to include additional locations if required to support survivors. The Government has estimated the number of Direct Lease properties required at approximately three hundred (300) housing units for this Contractor. If more properties are added to the Contractor's inventory that could be used for Direct Lease, the Contractor must provide an updated inventory to FEMA for evaluation if the additional properties are to be considered.

Properties should include existing residential properties for lease (e.g., corporate apartments, vacation rentals, and second homes) or any other type of residential property that meets (or can be made to meet) the standards identified in this Statement of Work (SOW). Properties may consist of multi-family dwellings, single family, duplexes, apartments, condominiums, townhouses, or readily fabricated dwellings. Units that are available to the general public that survivors can use Rental Assistance to lease are to not be included, along with any transient accommodations such as hotels and motels. The Contractor shall evaluate each property to ensure the property is safe, secure, and functional.

The Contractor shall not commence work under this SOW, unless a Direct Lease service request Blanket Purchase Agreement (BPA) is executed by the Contracting Officer (CO).

Below are specific tasks, items, and services to be completed by the Contractor, as required, for Direct Lease:

1. **Identify Properties.** The Contractor shall lease existing residential property not available to the general public (e.g., corporate apartments, vacation rentals, and second homes), and provide temporary housing for eligible individuals and households.
  - a. The Contractor may only lease properties that comply with federal, state, and local occupancy standards, to 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 by the property must be safe and functional. Safe means secure from disaster- related hazards or threats to occupants. Sanitary means free of disaster-related health hazards. Functional means an item or home capable of being used for its intended purpose.
- b. The Contractor shall evaluate properties according to the following factors:
    - i. Cost to the Federal Government: The Contractor shall lease properties at or below the established Fair Market Rent (FMR) from the Department of Housing and Urban Development (HUD) depicted in Figure 1 of this document.
    - ii. If the Contractor is unable to obtain sufficient units at the FMR, the Contractor shall notify the Contracting Officer's Representative (COR) in order for FEMA to review options and develop a solution.
    - iii. The Contractor shall ensure the property owner is capable of property management and the ability to provide maintenance services.
    - iv. The Contractor shall attempt to provide properties that are in a community with wrap- around services; such as, accessible public transportation, schools, fire and emergency services, grocery stores, and health care services.
  - c. The Contractor shall prioritize properties that include accessibility features or can easily be conformed to accessible requirements; and are in proximity to accessible public transportation. The monthly cost per unit may not exceed the amounts established in Figure 1 below, unless an increase is approved by FEMA.
    - i. FEMA will fund a one-time payment of security deposits for each unit, to be authorized and executed by the CO. The amount of each security deposit must not exceed the amount of one month of the authorized rent rate, and unused portions of each security deposit must be returned to FEMA upon release of the unit. In cases where a new applicant is leased into a unit previously occupied by a FEMA applicant, FEMA will pay a new security deposit if the previous applicant's deposit was utilized to cover cleanup or repairs. In situations where the security deposit does not cover the amount of damage to the unit, the occupant will be responsible to the property owner for the additional funds.
    - ii. The Contractor shall notify the COR for FEMA approval prior to leasing units consisting of four (4) or more bedrooms.
  - d. The Contractor shall implement and update a tracking spreadsheet for approved properties throughout the Direct Lease process. The tracking system must be approved by the COR prior to implementation. An example is provided at Attachment 2, Direct Lease Property Tracking Sheet.

***Figure 1- Maximum Monthly Rents***

County	1 BED	2 BED	3 BED	4 BED
Maui	\$ 1,606	\$ 1,986	\$ 2,731	\$ 2,944

2. **Property Inspections.** The Contractor shall inspect each property to ensure compliance with Federal, State and local occupancy standards prior to executing lease agreements with housing applicants. The Contractor shall provide FEMA verification that units meet HUD Housing Quality Standards (HQS) and received a formal screening. Each inspection will also verify property owner's capability to provide all property management services, including building maintenance.
3. **Contacting Applicants.** FEMA will identify eligible applicants for Direct Lease units and provide the following applicant information to the Contractor: applicant name, co-applicant names (if applicable), damage dwelling address, mailing address, phone numbers, and emails.
4. **Matching Applicants.** Once units are available, FEMA will initiate contact to the applicant within one (1) day and coordinate with the applicant to match the Direct Lease unit that fit the needs of the applicant. FEMA will also inform each applicant of the next steps towards their placement in a Direct Lease unit, such as having a background check for properties that require it.
  - a. The Contractor shall notify FEMA, within one (1) day, in each instance in regards to an applicant being denied by the property owner or leasing agent due to adverse information in their background check.
  - b. FEMA will not pay for background checks, credit checks, pet deposits, or application fees.
5. **Lease Agreements and Conditions.** The Direct Lease Contract Terms and Conditions, Attachment 4, is between FEMA and the Contractor or property owner; this document sets forth the terms of the Direct Lease contract including the use of the property and both parties' responsibilities. The property owner must agree to modify any lease between the property owner and the occupant to incorporate FEMA's program conditions of eligibility and termination of tenancy, through the Direct Lease Addendum (Attachment 6) to an existing lease the property owner may have or by using use the Direct Lease Occupant Lease Agreement (Attachment 5).
6. **Move-in of Applicants.** The Contractor and FEMA will be responsible for the move-in process for applicants into Direct Lease units. The Contractor 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. Prior to move- in, the Contractor shall provide the COR with the following documentation:
  - a. A copy of the inspection record confirming the property complies with Federal, State, and local occupancy standards; Attachment 3 has been provided as an example;
  - b. A copy of the Direct Lease Occupant Lease Agreement (Attachment 5) between



applicant and property owner. A property owner may use own tenant lease instead, but field counsel will need to review and approve. If there is any conflict between the terms in the owner's tenant lease and the Direct Lease Occupant Addendum (Attachment 6), the terms of the Direct Lease Occupant Addendum will prevail; and The Contractor is also responsible for providing executed copies of the Direct Lease Contract, Direct Lease Addendum, and Direct Lease Occupant Lease Agreement.

The COR is responsible for obtaining:

- a. A copy of the Direct Lease Contract (Attachment 4) that was completed in executing the lease agreement and specifies the monthly rent rates. The Direct Lease Occupant Lease Addendum (Attachment 6) is to be attached to the Direct Lease Contract.
  - b. A copy of the Direct Lease Temporary Housing Agreement (Attachment 7).
7. **Lease Agreement Payments.** The Contractor shall make rental payments to property owners in accordance with the rental or lease agreements for each property that is awarded under the BPA call/order. The Contractor shall make payments to property owners in a timely fashion.
8. **Terminate Lease Agreements.** FEMA will be responsible for any termination of assistance to applicants. The Contractor and property owners shall be responsible for eviction and removal of applicants whose assistance has been terminated by FEMA. Property owners may receive reimbursement for reasonable costs associated with the eviction process; eviction costs reimbursement and time period for these costs will be established between the Contractor and FEMA within the contract. FEMA may terminate the lease for the housing unit by providing the Contractor with a written thirty (30) calendar day Decision to Terminate Notice to Property Owner (Attachment 8). FEMA will also charge the applicant penalty fees directly for the time they continue to stay in a unit past their termination of assistance.
9. **Utilities.** The Government is not responsible for utilities, unless utilities are included in the monthly rental fee and do not exceed the established monthly rental rates established in Figure 1. Applicants are responsible for obtaining their own utility accounts.
10. **Access and Functional Needs.** A provision allowing the property owner to make, at FEMA's expense, 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 incurrence of costs. All modifications or improvements are considered permanent and FEMA is not responsible for removing modifications or improvements upon completion of the lease agreement.
11. **Government Equipment.** There will be no government-furnished equipment provided to the Contractor. The Contractor will not have access to FEMA's GES.
12. **Safeguarding and Info Sharing. Information Sharing.** To accomplish the tasks outlined in this contract, FEMA will share with the contractor the following PII data elements: name, damaged dwelling address, mailing address, phone number, and email address. The information sharing outlined in this contract is covered in the following Privacy Impact

## **Responsibilities**

### **Need to Know**

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

### **Prohibition on Computer Matching**

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

### **Recipient Requirement**

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

## **SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)**

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

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

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

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN),

email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

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

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

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

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

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint,



voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

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

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

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

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

<http://csrc.nist.gov/publications/PubsSPs.html>

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

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

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

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

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

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

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

(i) Security Authorization Process Documentation. SA documentation shall be developed



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

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

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

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

(1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting

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

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

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

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

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

requirements for Contractor systems.

*(f) Sensitive Information Incident Reporting Requirements.*

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

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

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;



(xiii) Number of people potentially affected, and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

*(g) Sensitive Information Incident Response Requirements.*

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

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

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

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews, and

(iv) Data analyses and processing.

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

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

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

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

(i) A brief description of the incident;

(ii) A description of the types of PII and SPII involved;

- (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
- (iv) Steps individuals may take to protect themselves;
- (v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- (vi) Information identifying who individuals may contact for additional information.
- (i) *Credit Monitoring Requirements.* In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:
  - (1) Provide notification to affected individuals as described above; and/or
  - (2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:
    - (i) Triple credit bureau monitoring;
    - (ii) Daily customer service;
    - (iii) Alerts provided to the individual for changes and fraud; and
    - (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or
  - (3) Establish a dedicated call center. Call center services shall include:
    - (i) A dedicated telephone number to contact customer service within a fixed period;
    - (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
    - (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
    - (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
    - (v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
    - (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.
- (j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

## INSPECTION

Properties are subject to inspection by FEMA and other applicable Government agencies. The Contractor shall participate in responding to all requests for information and inspection or review findings by regulatory agencies. The Contractor shall allow FEMA, or an entity or organization approved by FEMA, to conduct inspections of rental units, as required, to ensure an acceptable level of services and acceptable conditions of housing as determined by FEMA. No notice to the Contractor is required prior to an inspection. FEMA will share findings of the inspection with the Contractor (See Attachment 3).

#### **QUALITY ASSURANCE/QUALITY CONTROL PROVISIONS**

The Contractor shall adhere to all quality assurance/quality control provisions outlined in the Quality Assurance Surveillance Plan. (See Attachment 1).

#### **PLACE OF PERFORMANCE**

Within a 50-mile radius of Maui County, HI.

#### **PERIOD OF PERFORMANCE**

18 Months

#### **GOVERNMENT POINTS OF CONTACT:**

CONTRACTING OFFICER



CONTRACTING OFFICER REPRESENTATIVE



#### **APPLICABLE ATTACHMENTS:**

1. Quality Assurance Surveillance Plan (QASP)
2. Direct Lease Property Tracking Sheet
3. Direct Lease Property Inspection Checklist
4. Direct Lease Contract
5. Direct Lease Occupant Lease Agreement
6. Direct Lease Occupant Lease Addendum
7. Direct Lease Temporary Housing Agreement
8. Decision to Terminate Notice to Property Owner
9. Fair Market Rate – Maui County



10. Furniture Checklist
11. Pricing CLIN Structure Spreadsheet