

Federal Emergency Management Agency



STATEMENT OF OBJECTIVE (SOO) FOR:

OCFO Financial Management Division,
Corrective Action and Audit Remediation Support Services

Janine Bennett, Contracting Officer

PROCUREMENT SENSITIVE INFORMATION

This document contains non-public information intended for
use on a need-to-know basis within FEMA only.

Please protect this document as procurement sensitive and handle accordingly.

DEPARTMENT OF HOMELAND SECURITY (DHS)

Statement of Objectives (SOO) For Corrective Action Implementation and Audit Remediation Support

Purpose

The purpose of this effort is to obtain contractor support services to assist the FEMA Office of the Chief Financial Officer (OCFO) Financial Management Division (FMD), Risk Management and Compliance (RMC) Branch, with corrective action implementation and remediation of identified internal control deficiencies, audit findings, Mission Action Plans, Plans of Action and Milestones, and related financial, operational, IT, risk, and compliance issues.

The contractor shall support FEMA in strengthening its internal control environment, addressing financial and operational control deficiencies, improving audit readiness, supporting corrective action implementation, and documenting remediation efforts in accordance with applicable federal requirements, including OMB Circular A-123, GAO Standards for Internal Control in the Federal Government, and DHS and FEMA policies. The objective of this requirement is focused on corrective action implementation and remediation support after deficiencies, findings, risks, and/or compliance issues have been identified through audits, assessments, monitoring, management reviews, and/or other oversight activities. This support is to assist the FMD, but other FEMA Offices and Programs may utilize these services to meet the intent of the objective.

***Note:** Routine internal control assessment, recurring compliance monitoring, baseline control testing, and A-123 testing activities are outside the primary scope of this requirement and are expected to be addressed through a separate Internal Control and Compliance Support Services requirement. This separation is intended to preserve clarity of roles, reduce overlap between assessment and remediation activities, and ensure objectivity in FEMA's internal control and compliance environment.*

Scope

The scope of this effort is to provide technical, analytical, program management, documentation, reporting, and advisory support to help FEMA plan, implement, monitor, and document remediation activities.

Support may span FEMA's financial management, disaster assistance, grants, insurance-related, property, human capital, information technology, and mission support processes, but only where corrective action implementation or remediation support is required for previously identified deficiencies, findings, or risks.

This effort includes coordination across OCFO, FEMA program offices, process owners, system owners, and other stakeholders to support timely, effective, and sustainable remediation of identified deficiencies and audit findings in alignment with OMB Circular A-123, GAO Standards for Internal Control in the Federal Government, federal financial management requirements, DHS policy, and FEMA guidance.

Period of Performance

The period of performance for this statement of objectives is one 12-month base period with four 12-month option periods for a total of five years if all options are exercised at the discretion of the government.

Place of Performance

The primary place of performance will be the Contractor's facilities or at FEMA Headquarters—500 C Street SW, Washington, DC 20024, or at 430 Market St. Winchester, Virginia.

- Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulation. The Contractor shall be responsible for obtaining COR approval (email is acceptable) for all reimbursable travel in advance of each travel event.
- The Contractor will not be reimbursed for local travel to and from FEMA Headquarters, Winchester, VA, or within the National Capital Region (NCR).
- The Contractor is authorized to telework at the discretion of the Contract Officer Representative (COR).

Background

FEMA plays a critical role in the nation's emergency management framework by coordinating federal preparedness, response, recovery, and mitigation efforts before, during, and after disasters. FEMA's mission is delivered through a large and complex operating environment that includes more than 21,000 employees, coordination with state, local, tribal, and territorial partners. FEMA also administers high-volume, high-impact programs, including disaster assistance, grants, and insurance-related activities, while also managing substantial disaster obligations and long-term recovery funding.

The FEMA Office of the Chief Financial Officer manages and oversees FEMA's fiscal resources in accordance with applicable laws, policies, and guidance. Within OCFO, the Financial Management Division oversees FEMA's financial controls, operations, policy, and financial statement activities. The RMC Branch develops FEMA's internal controls program, manages the annual financial statement audit, performs OMB Circular A-123 transaction and IT general control testing, and works with FEMA offices and programs to remediate identified deficiencies.

FEMA's emergency management mission creates a fiscal environment characterized by significant transaction volume, disaster-driven surge requirements, long-term recovery obligations, interagency coordination, compliance requirements, and heightened public stewardship expectations. Sustained remediation support is needed to help FEMA address internal control deficiencies, audit findings, corrective action plans, Mission Action Plans, IT-related Plans of Action and Milestones, and related financial, operational, and compliance risks while maintaining alignment with OMB Circular A-123, GAO Standards for Internal Control in the Federal Government, federal financial management requirements.

Performance of Objectives

Outcome-oriented support for non-personnel services is needed to assist FEMA OCFO RMC in strengthening FEMA's internal control environment and remediating internal control deficiencies, audit findings, corrective action plans, Mission Action Plans, Plans of Action and Milestones, and related financial, operational, IT, and compliance risks.

The contractor's approach shall support FEMA's compliance with applicable federal financial management, internal control, audit, payment integrity, and IT control requirements, including the DHS Financial Accountability Act, Chief Financial Officers Act, Federal Financial Management Improvement Act, Federal Managers' Financial Integrity Act, OMB Circular A-123, Payment Integrity Information Act of 2019, NIST Special Publication 800-53, Federal Information System Controls Audit Manual, GAO Standards for Internal Control in the Federal Government, and other applicable DHS and FEMA policy, guidance, laws, and regulations.

The contractor shall provide qualified personnel with expertise in federal financial management, accounting, internal controls, audit remediation, IT controls, financial systems, data quality, and related compliance requirements. The contractor shall be capable of supplementing FEMA staff throughout the fiscal year, including during audit cycles, reporting periods, remediation milestones, and other high-priority periods requiring sustained or ad hoc support.

The contractor shall propose a solution that achieves the following objectives:

1. Corrective Action and Remediation Planning

FEMA requires timely, actionable, and sustainable remediation plans for identified internal control deficiencies, audit findings, Mission Action Plans, and IT-related Plans of Action and Milestones. The contractor's solution should improve FEMA's ability to define root causes, milestones, risks, dependencies, responsible parties, critical path activities, performance measures, resource considerations, and measurable remediation outcomes. The solution should also incorporate lessons learned from prior audits, assessments, and remediation activities.

2. Remediation of Business Process and Internal Control Findings

FEMA requires support to remediate business process findings, internal control deficiencies, material weaknesses, significant deficiencies, reportable conditions, and other control issues. The contractor's solution should strengthen control design, improve business processes, support internal controls over financial reporting and operations, reduce recurrence of findings, and support alignment with GAO Standards for Internal Control in the Federal Government.

3. Remediation of IT Control Findings and System-Related Risks

FEMA requires support to remediate IT control findings and system-related risks affecting financial reporting, operational controls, data quality, security, system interfaces, and compliance. The contractor's solution should support improvements to IT general controls, application controls, system-related control documentation, financial system controls, and IT-related remediation plans in alignment with applicable federal, DHS, and FEMA requirements.

4. Business Process, Reporting, and Data Quality Improvements

FEMA requires process improvement support to strengthen financial management, reporting, data quality, reconciliation, and compliance-related controls. The contractor's solution should support improvements to

business processes, control design, financial systems conformance, DATA Act-related controls, and other reporting or data quality requirements applicable to FEMA's financial management environment.

5. Testing, Verification, and Validation of Remediation Efforts

FEMA requires support, as authorized by the Government, to determine whether remediation actions address identified deficiencies, are appropriately designed, operate as intended, and are ready for management review or audit follow-up. The contractor's solution should provide a risk-based approach to testing, verification, validation, evidence review, and reporting of remediation results, including identification of remaining risks and potential mitigation options.

Testing, verification, and validation under this requirement is focused on determining whether corrective actions and remediation activities have addressed previously identified deficiencies, findings, or risks. This requirement is not intended to perform routine A-123 assessment testing or recurring internal control monitoring covered under a separate internal control and compliance support requirement.

6. Reporting, Tools, and Management Insight

FEMA requires timely and actionable information on remediation status, risk areas, recurring issues, aging items, dependencies, impediments, and progress against corrective action milestones. The contractor's solution should improve management visibility through effective use of project plans, tracking tools, dashboards, status reporting, executive briefings, decision documents, and other management reporting products.

7. Technical Assistance and Stakeholder Coordination

FEMA requires technical assistance and coordination across OCFO, program offices, process owners, system owners, and other stakeholders to advance remediation activities and align efforts with FEMA and DHS timelines. The contractor's solution should improve communication, accountability, issue resolution, milestone monitoring, and integration of remediation activities across FEMA, including support for ad hoc IT and non-IT internal control requests.

8. Adaptability to New Requirements

FEMA requires remediation support that can adapt to new or changing requirements issued through laws, regulations, executive direction, OMB guidance, DHS policy, FEMA guidance, audit recommendations, or other governing bodies. The contractor's solution should help FEMA assess the impact of new requirements on internal controls, remediation priorities, documentation, reporting, and compliance activities.

9. Sustainable Improvements and Knowledge Transfer

FEMA requires remediation support that promotes sustainable improvements beyond the period of contractor performance. The contractor's solution should include approaches for guidance, training, templates, standard operating procedures, resource materials, user support, and knowledge transfer to support consistent remediation practices and long-term control effectiveness.

Performance Expectations

The contractor shall propose an approach that supports timely, accurate, and high-quality remediation support throughout the fiscal year and audit cycle. The proposed approach should address how the contractor will meet FEMA and DHS deadlines, support time-sensitive audit and remediation milestones, respond to ad hoc internal control requests, maintain quality control over deliverables, minimize rework, identify risks and dependencies, and provide actionable reporting and recommendations to support FEMA management.

Operating Constraints

- Flexibility is required to support this requirement due to FEMA's evolving emergency management mission, disaster-driven surge requirements, complex financial management environment, ongoing remediation priorities, and changing audit and compliance needs.
- FEMA is modernizing its core financial, procurement, and asset management systems, with the transition anticipated in early FY 2027. The contractor shall account for this transition in its remediation support approach, including potential impacts to internal controls, business process documentation, data quality, reporting, system-related corrective actions, stakeholder coordination, and continuity of remediation activities.
- The contractor shall perform work only within the scope of the applicable requirement. The Government may maintain separate requirements for internal control assessment and compliance support and for corrective action and audit remediation support. The contractor shall identify any actual, potential, or perceived overlap, independence concern, or organizational conflict of interest that may arise between assessment, testing, remediation, and validation activities and shall notify the Contracting Officer (CO), Contracting Officer Representative (COR), and FEMA Program Manager in accordance with contract requirements.
- The contractor shall perform all work in accordance with applicable federal laws, regulations, standards, DHS policy, FEMA guidance, and contract requirements, including OMB Circular A-123, GAO Standards for Internal Control in the Federal Government, and applicable federal financial management requirements.
- The scope of work excludes acquisition support, source selection activities, and inherently governmental functions. The contractor shall not access source selection sensitive information; perform acquisition strategic planning, requirements development, acquisition portfolio management, or evaluation support; or otherwise influence the outcome of any current or future procurement.
- The contractor shall not influence, determine, approve, or direct FEMA budget allocations, funding decisions, or budget alignments. FEMA retains responsibility for all management decisions, including approval of corrective actions, acceptance of risk, operation of controls, management assertions, and final determination of remediation status.

Applicable Documents or References

The contractor shall perform work in accordance with applicable laws, regulations, standards, policies, and guidance, including but not limited to:

- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control

- GAO, Standards for Internal Control in the Federal Government
- Federal Managers' Financial Integrity Act
- Chief Financial Officers Act
- Federal Financial Management Improvement Act
- DHS Financial Accountability Act
- Payment Integrity Information Act of 2019
- Federal Information System Controls Audit Manual
- NIST Special Publication 800-53, as applicable

Additional materials required to perform the work will be provided to the contractor after award, as appropriate and subject to applicable access, security, privacy, and information protection requirements. These materials may include, but are not limited to, applicable Department and Agency governing documents, financial management policies, guidance, templates, procedures, and other reference materials.

Appendix D: Information Sharing

The tasks outlined in this contract require access to the FEMADEx system; however, they do **not** require access to the PII or SPII contained within FEMADEx.. The FEMADEx Privacy Threshold Analysis (PTA) is currently expired and in process of being renewed. The deliverables within this scope of work do not extend beyond MS suites and Enterprise Business Enablement. There will be no access of PII/SPII beyond first name, last name, email addresses of FEMA employees from Outlook. In addition, once a solution is planned/developed within FEMADex the Program Office will work with FEMA Privacy to have the Privacy Threshold Analysis (PTA) completed.

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

- FEMADex PIA in development
- DHS/FEMA/PIA-013 Grant Management Programs
- DHS/ALL/PIA-015 DHS Web Portals
- DHS/FEMA/PIA-040 Deployment Tracking System
- DHS/FEMA/PIA-052 Grants Management Modernization
- DHS/ALL/PIA-014 Personal Identity Verification Management
- DHS/ALL/PIA-038 Integrated Security Management System
- DHS/ALL/PIA-043 Talent Acquisition
- DHS/ALL/PIA-050 Trusted Identity Exchange
- DHS/ALL/PIA-053 DHS Financial Management Systems
- DHS/FEMA/PIA-049 Individual Assistance Program
- DHS/ALL/PIA-006 DHS General Contacts List
- DHS/FEMA/PIA-011 National Flood Insurance Program
- DHS/FEMA/PIA-026 Operational Data Store (ODS) and Enterprise Data Warehouse (EDW),
- DHS/FEMA/PIA-048 National Flood Insurance Program Direct Servicing Agent System

Interim coverage is provided through the above PIAs that cover the source systems. Once the system is closer to production, PRIV expects that FEMA will draft and submit a new PIA for the FEMADex Program. No SORN coverage is required as information is not retrieved by a unique identifier.

To accomplish the tasks outlined in this contract, FEMA will provide the contractor access to PII of first name, last name, email addresses, and work phone numbers of FEMA employees via Global Address List (GAL) and Enterprise Business Enablement (formerly Microsoft Office 365) applications by way of FEMA laptop use. The information sharing is authorized by Routine Use F of the following Systems of Records Notices: DHS/ALL-014 Department of Homeland Security Personnel Contact Information, March 16, 2018 83 FR 11780, DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792, DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, November 25, 2008, 73 FR 71659.

The information sharing is also covered by the following Privacy Impact Assessments: DHS/ALL/PIA-015 Web Portal and DHS/ALL/PIA-059 Employee Collaboration Tool.

Need to Know

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

Prohibition on Computer Matching

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

Return or Destruction of Data when no longer needed

If at any time during the term of this contract any part of FEMA PII, in any form, that the Contractor obtains from FEMA ceases to be required by the Contractor for the performance of the contract, or upon 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.

Appendix E: 52.224-1 Privacy Act Notification

Privacy Act Notification (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 ([5 U.S.C. 552a](#)) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

Appendix F: 52.224-2 Privacy Act

Privacy Act (APR 1984)

(a) The Contractor agrees to-

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies-

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)

(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

Appendix G: H-1 HSAR DEV 15-01B Information Technology Security and Privacy 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 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.

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

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

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

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

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

(7) Information Systems Vulnerability Information (ISVI) means:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Incident means an occurrence that—

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

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

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

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

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

(b) Handling of Controlled Unclassified Information.

- (1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>.

- (2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.
- (3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.
- (4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) *Incident Reporting Requirements.*

- (1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.
- (2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.
- (3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.
- (4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.
- (5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:
 - (i) Unique Entity Identifier (UEI);
 - (ii) Contract numbers affected unless all contracts by the company are affected;
 - (iii) Facility CAGE code if the location of the event is different than the prime Contractor location;

- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);
- (v) Contracting Officer POC (address, telephone, and email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms, or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the government PII or SPII contained within the system; and
- (xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

- (1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.
- (2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of incidents.
- (3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:
 - (i) Inspections;
 - (ii) Investigations;
 - (iii) Forensic reviews;
 - (iv) Data analyses and processing; and
 - (v) Revocation of the Authority to Operate (ATO), if applicable.
- (4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.
- (5) The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

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

(f) *Other Reporting Requirements.* Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may

apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

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

HSAR 3052.240-72 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION ALT I (JULY 2023) (HSAR DEVIATION 25-12) (Effective November 3, 2025)

(h) *Authority to Operate.* The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) Complete the Security Authorization process. The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems (Version 13.3, February 13, 2023), or any successor publication; and the Security Authorization Process Guide, including templates. These policies and templates are accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>.

- (i) Security Authorization Package. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package 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). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.
- (ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the information 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 SP 800–53, Security and Privacy Controls for Information Systems and Organizations, or successor publication, accessible at <https://csrc.nist.gov/publications/sp>. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

- (i) Updating the SA package in the DHS Information Assurance Compliance System; or
- (ii) Submitting the updated SA package directly to the COR.

(3) Security Review. The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), 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) Federal Reporting and Continuous Monitoring Requirements. Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

Appendix H: H-2 HSAR DEV 15-01A Safeguarding of Sensitive 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:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, “Chemical Facility Anti-Terrorism Standards,” and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual “Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information” dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII’s implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, “Protection of Sensitive Security Information,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, “Sensitive Security Information (SSI)” and, within the Transportation Security Administration, TSA MD 2810.1, “SSI Program”;

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal,

territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

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

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

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

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

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

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, 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;
- (D) Ethnic or religious affiliation;
- (E) Sexual orientation;
- (F) Criminal history;
- (G) Medical information; and
- (H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance

ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

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

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

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

Incident means an occurrence that—

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

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

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

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

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

(b) Handling of Controlled Unclassified Information.

- (1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies

and procedures are accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

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

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) Incident Reporting Requirements.

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

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

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels.

When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

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

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, Incident Response, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

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

(d) Incident Response Requirements.

- (1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.
- (2) The Contractor shall provide full access and cooperation for all activities

determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of incidents.

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

- (i) Inspections;
- (ii) Investigations;
- (iii) Forensic reviews;
- (iv) Data analyses and processing; and
- (v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

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

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

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

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

Alternate I

(h) *Authority to Operate.* The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems* (Version 13.3, February 13, 2023), or any successor publication; and the *Security Authorization Process Guide*, including templates. These policies and templates are accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>.

(i) *Security Authorization Package.* The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package 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). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment.* Contractors shall have an independent third party validate the security and privacy controls in place for the information 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 SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at <https://csrc.nist.gov/publications/sp>. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

- (i) Updating the SA package in the DHS Information Assurance Compliance System; or
- (ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole

discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), 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) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at <https://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

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

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

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

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

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

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

(b) *PII and SPII Notification Requirements.*

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either

under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

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

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

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

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

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

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

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

(3) Establish a dedicated call center. Call center services shall include:

- (i) A dedicated telephone number to contact customer service within a fixed period;
- (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
- (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

- (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
- (v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
- (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

Privacy Training – Alternate I (DEVIATION)

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

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

- (1) Have access to a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
- (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing Privacy at DHS: Protecting Personal Information accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

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

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

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, “Chemical Facility Anti-Terrorism Standards,” and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual “Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information” dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII’s implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, “Protection of Sensitive Security Information,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, “Sensitive Security Information (SSI)” and, within the Transportation Security Administration, TSA MD 2810.1, “SSI Program”;

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- (g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.
- (h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.
- (i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).
- (j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.
- (k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:
 - There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
 - The waiver must be in the best interest of the Government.
- (l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

Appendix I: 52.204-9 Personal Identity Verification of Contractor Personnel

Personal Identity Verification of Contractor Personnel (Jan 2011)

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

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

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

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

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

Appendix J: Security Training Requirements

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

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 (COR), before the contractor or subcontractor is granted access to classified or unclassified information but no later than thirty (30) calendar days after EOD onboarding is completed. Send certificates of completion for Unauthorized Disclosure, OPSEC, and Insider Threat to the FEMA COR no later than thirty (30) calendar days after onboarding of contractors for contract is completed. New employees entering the contract must receive the briefing within ten (10) business days of joining the contract.

Unauthorized Disclosure of Classified or Unclassified Information

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

Access to the training can be obtained at:

<https://securityawareness.usalearning.gov/disclosure/index.html>

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:

<https://securityawareness.usalearning.gov/opsec/index.htm>

Insider Threat Training

The Department of Homeland Security (DHS) requires that Contractor employees take an annual Insider Threat Training course. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award or new employees entering the contract and be completed on an annual basis thereafter not later than October 31st of each year.

Insider Threat training for contractors can be found at:

<https://securityawareness.usalearning.gov/itawareness/index.htm#>

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 shall:

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

Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.

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.

Appendix K: Records Management Compliance Clauses and Training Requirement

Records Management Obligations:

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.

Definitions

“Federal record” as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

includes FEMA records;

does not include personal materials;

applies to records created, received, or maintained by Contractors pursuant to their FEMA contract; and

may include deliverables and documentation associated with deliverables

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 of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5

U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

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 PWS. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to FEMA control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the PWS. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

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.

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.

Records Management Training

The Department of Homeland Security (DHS) requires that Contractor employees take an annual Records Management for Everyone course. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award or new employees entering the contract and be completed on an annual basis thereafter not later than October 31st of each year.

Records Management for Everyone training for contractors can be found at:

<https://fekc.fema.net/ContentDetails.aspx?id=2D865111E0C54088BDF68EA8414C286F>

Contractors need to complete the FEKC Account form and send it to FEMA-FEKC@fema.dhs.gov to receive 30-day FEKC account access to complete the mandatory training.

Appendix L: Section 508 Compliance

SECTION 508 - ELECTRONIC AND INFORMATION TECHNOLOGY

Section 508 of the Rehabilitation Act (classified to [29 U.S.C. § 794d](#)) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at <https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5>. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018, and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

1.1 Section 508 Requirements for Technology Services

When providing installation, configuration or integration services for ICT, the Contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.

When modifying, installing, configuring, or integrating commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.

When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at <https://www.dhs.gov/compliance-test-processes>.

When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting

test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under “Accessibility Tests for Documents”, which are published at <https://www.dhs.gov/compliance-test-processes>. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at <https://www.dhs.gov/trusted-tester>

Contractor personnel shall possess the knowledge, skills, and abilities necessary to address the accessibility requirements in this work statement.

1.2 Section 508 Deliverables

Section 508 Test Plans: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.

Section 508 Test Results: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

Section 508 Accessibility Conformance Reports: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at <https://www.itic.org/policy/accessibility/vpat>. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

Other Section 508 Documentation: The following documentation shall be provided upon request for ICT items offered through this contract:

Documentation of features provided to help achieve accessibility and usability for people with disabilities.

Documentation on how to configure and install the ICT Item to support accessibility.

Documentation of core functions that cannot be accessed by persons with disabilities.

Documentation of remediation plans to address non-conformance to the Section 508 standards.

Appendix M: 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 shall undergo a Tier 1 (T1) background investigation which is equivalent to the previously identified National Agency Check with Inquiries (NACI). Either of these investigations must be supported by a separate credit check and must receive a favorable adjudication thereof from FEMA PSD prior to holder performing work under this contract. A favorably adjudicated NACI & C will remain acceptable for the purpose of reciprocity where a T1 investigation is required for a period of five (5) years from the date of completion and favorable adjudication provided that all other requirements for the application of reciprocity are met.

Low Risk with Information System Access

Contractor personnel occupying positions or performing functions with a moderate risk designation shall undergo a Tier 2 Suitability (T2S) background investigation which is equivalent to the previously identified Moderate Risk Background Investigation (MBI) and must receive a favorable adjudication thereof from FEMA PSD prior to the holder performing work under this contract. A favorably adjudicated MBI will remain acceptable for the purpose of reciprocity where a T2S investigation is required for a period of five (5) years from the date of completion and favorable adjudication provided that all other requirements for the application of reciprocity are met.

Moderate Risk

Contractor personnel occupying positions or performing functions with a moderate risk designation shall undergo a Tier 2 Suitability (T2S) background investigation which is equivalent to the previously identified Moderate Risk Background Investigation (MBI) and must receive a favorable adjudication thereof from FEMA PSD prior to the holder performing work under this contract. A favorably adjudicated MBI will remain acceptable for the purpose of reciprocity where a T2S investigation is required for a period of five (5) years from the date of completion and favorable adjudication provided that all other requirements for the application of reciprocity are met.

High Risk

Contractor personnel occupying positions or performing functions with a high-risk designation shall undergo a Tier 4 (T4) background investigation which is equivalent to the previously identified Background Investigation (BI), and must receive a favorable adjudication thereof from FEMA PSD prior to the holder performing work under this contract. A favorably adjudicated BI will remain acceptable for the purpose of reciprocity where a T4 investigation is required for a period of five (5) years from the date of completion and favorable adjudication provided that all other requirements for the application of reciprocity are met.

Background Investigation Process

Contractors performing on this contract must be United States Citizens. Contractor applicants must also be 18 years of age or older to allow for the conduct of certain security related queries.

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

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

the investigation was completed within the last five (5) 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 to the contractor personnel that contains the following documents, which are incorporated into this contract by reference, along with a link

to the Office of Personnel Management's Electronic Questionnaires for Investigation Processing (e-QIP) system and instructions for submitting the necessary information:

Standard Form 85P, "Questionnaire for Public Trust Positions"

Optional Form 306, "Declaration for Federal Employment"

SF 87, "Fingerprint Card" (2 copies)

DHS Form 11000-6, "Non-Disclosure Agreement"

DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

Applicants born outside the United States will be required to provide proof of citizenship in the form of a Certificate of Naturalization (Form N550 or N570), an unexpired U.S. Passport, or State Department issued Consular Report of Birth Abroad (CRBA) (FS-240).

FEMA PSD will only accept complete packages consisting of all of the above document and Standard Form 85P, which must be completed electronically through the Office of Personnel Management's e-QIP system. The Contractor is responsible for ensuring that all contractor personnel timely and properly submit all required background information.

Residency requirements apply to the background investigation process. Persons subject to investigation and final adjudication for fitness or suitability must have lived within the United States for no less than three (3) of the last (five) 5 years as defined in the DHS Instruction 121-01-007-01, *The Department of Homeland Security, Personnel Security, Suitability and Fitness Program* (June 14, 2016). DHS has determined this to be the amount of time required to be the sufficient minimum investigative period for the purpose of performing a suitability or fitness adjudication. Both, OPM and OMB require a final adjudicative decision to support the issuance of the HSPD-12 compliant PIV Card that contractors are issued by FEMA Physical Security.

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

perform work under this contract upon completion of and final adjudication of the full background investigation.

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

Continued Eligibility and Reinvestigation

Eligibility determinations based on a T1, T2S, or T4 (or the equivalent OPM investigation) are valid for five (5) 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.

Appendix N: 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.

Appendix O: 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.

Appendix P: Separation from Contract

The Contractor shall notify the FEMA COR of all terminations/resignations within five (5) 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.

Recipient Requirement - Return or Destruction of Data when no longer needed

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

Appendix Q: OCIO CISO Cyber-Supply Chain Risk Management (C-SCRM)

a. Definitions

i. Component: a unit defined by the supplier that connects to and functions as part of the product. For software products, a component is a unit of software defined by a supplier at the time the component is built, packaged, or delivered. For hardware, a component is one hardware unit designed to connect to and function as part of a larger product.

ii. End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

iii. End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

iv. Information and Communications Technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

v. Product: part of the equipment (hardware, software, and materials) for which usability is to be specified or evaluated.

b. Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product

i. The contractor shall provide new equipment unless otherwise formally approved by the Government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the Government. In the event that a shipped OEM product, or part or component of that product, fails, all replacements must be new (i.e., non-refurbished, not previously used) OEM.

ii. The contractor may provide previously-used OEM products only with written Government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

c. Accounting of Components in ICT Products

- i. The contractor shall provide and maintain a list of components for each product used in performance of the contract, including through subcontracts or other arrangements. This list for each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.
- ii. The contractor shall notify the Government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to reflect the new version of the software. This includes software builds to integrate an updated component or dependency.
- iii. For software products, the contractor shall provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract and replaced when End of Support (EoS) is reached.
- iv. A contractor using team members in performance of the contract (e.g., subcontractors or other service providers) shall ensure that the standards for the accounting of components in this subsection are met by team members.

d. Supply-Chain Transport

- i. The contractor shall use formal, documented, and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.
- ii. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance and make available for inspection upon request of the Government.
- iii. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.
- iv. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.
- v. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being

shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Changes to Ownership and Control

i. The Contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any significant changes to corporate ownership or control from contract award through final delivery or the end of the period of performance. A significant change would be one in which a change occurs in the individuals or entities who, directly or indirectly, either (1) exercises substantial control over an entity, or (2) owns or controls at least 25 percent of the ownership interests of an entity.

Appendix R: FedRAMP Certified

The proposed cloud solution must be FedRAMP certified.

Reference: Federal Risk and Authorization Management Program (FedRAMP), <http://www.fedramp.gov>:

National Institute of Standards and Technology (NIST), U.S. Department of Commerce (DOC), Special Publication (SP) 500-292, *NIST Cloud Computing Reference Architecture*, September 2011.

NIST, U.S. DOC, SP 800-145, *NIST Definition of Cloud Computing*, September 2011.

Cloud computing. All use of cloud computing products or services that process unclassified information must comply with the FedRAMP Authorization Act, 44 U.S.C. Section 3607 et. seq. The following requirements apply when using cloud computing to provide information systems or services in the performance of the contract.

Cloud computing security requirements. The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with FedRAMP Security Authorization Requirements unless notified by the Contracting Officer that this requirement has been waived by the Agency Chief Information Officer.

Cloud computing continuous monitoring. The Contractor shall maintain an adequate continuous monitoring capability based on the FedRAMP Security Authorization Requirements including processes described in the NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations and governed by the FedRAMP Continuous Monitoring Strategy Guide.

Cloud computing services cyber incident reporting. The Contractor shall report all cybersecurity incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted according to FedRAMP Security Authorization Requirements, published FedRAMP Incident Communications Procedures, and Federal Incident Notification Guidelines for submitting incident notifications to CISA using the CISA incident reporting form (<https://us-cert.cisa.gov/report>).

Appendix S: DHS Geospatial Information System Compliance

All implementations that require access to the DHS Geospatial Information Infrastructure (GII), including geospatial data, information, and services shall comply with the applicable policies and requirements set forth in the GII, including (but not limited to) the following:

- All data built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Data Reference Model.
- All software built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Technical Reference Model

Appendix T: Enterprise Architecture

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

All developed solutions and requirements shall be compliant with the HLS EA.

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

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Architecture Division (EAD) for review, approval and insertion into the DHS Data Reference Model and Mobius.

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

Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Appendix U: Artificial Intelligence / Machine Learning

Artificial Intelligence / Machine Learning Requirements Definitions: Artificial Intelligence (AI) includes the following:

- (1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
 - (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
 - (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
 - (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task.
 - (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.
- Requirements: The 2019 National Defense Authorization Act (NDAA) and Executive Order (EO) 13960 require that AI used in the Federal Government foster public trust and confidence while protecting privacy, civil rights, civil liberties, and American values. All federal employees, contractors, and subcontractors, when designing, developing, acquiring, and/or using AI for or within DHS, will adhere to the following 9 principles.
1. Lawful and respectful of our Nation's values: Agencies shall design, develop, acquire, and use AI in a manner that exhibits due respect for our Nation's values and is consistent with the Constitution and all other applicable laws and policies, including those addressing privacy, civil rights, and civil liberties.
 2. Purposeful and performance-driven: Agencies shall seek opportunities for designing, developing, acquiring, and using AI, where the benefits of doing so significantly outweigh the risks, and the risks can be assessed and managed.
 3. Accurate, reliable, and effective: Agencies shall ensure that their application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective.
 4. Safe, secure, and resilient: Agencies shall ensure the safety, security, and resiliency of their AI applications, including resilience when confronted with systematic vulnerabilities, adversarial manipulation, and other malicious exploitation.
 5. Understandable: Agencies shall ensure that the operations and outcomes of their AI applications are sufficiently understandable by subject matter experts, users, and others, as appropriate.

6. Responsible and traceable: Agencies shall ensure that human roles and responsibilities are clearly defined, understood, and appropriately assigned for the design, development, acquisition, and use of AI. Agencies shall ensure that AI is used in a manner consistent with these Principles and the purposes for which each use of AI is intended. The design, development, acquisition, and use of AI, as well as relevant inputs and outputs of particular AI applications, should be well documented and traceable, as appropriate and to the extent practicable.

7. Regularly monitored: Agencies shall ensure that their AI applications are regularly tested against these Principles. Mechanisms should be maintained to supersede, disengage, or deactivate existing applications of AI that demonstrate performance or outcomes that are inconsistent with their intended use or this order.

8. Transparent: Agencies shall be transparent in disclosing relevant information regarding their use of AI to appropriate stakeholders, including the Congress and the public, to the extent practicable and in accordance with applicable laws and policies, including with respect to the protection of privacy and of sensitive law enforcement, national security, and other protected information.

9. Accountable: Agencies shall be accountable for implementing and enforcing appropriate safeguards for the proper use and functioning of their applications of AI, and shall monitor, audit, and document compliance with those safeguards. Agencies shall provide appropriate training to all agency personnel responsible for the design, development, acquisition, and use of AI.