As of 03/31/2026

TRANSPORTATION SECURITY ADMINISTRATION GOLD+

Terms & Conditions

1.0 Terms and Conditions

1.2 Cybersecurity Policy for TSA Government Acquisitions (November 2025)

A. General Security Requirements:

A.1. Special notice for program sponsors:
The following Cybersecurity policy requirements supersedes any inadvertent or deliberate contradiction in previous sections of this document. Program sponsors must ensure this section is thoroughly reviewed prior to initiating the *Appendix G* approval process.

A.2. All authorized, cleared and vetted personnel (i.e., federal employees; and primary, subcontractor, and/or 3rd party vendors or contractors) supporting or doing business per agreement with TSA (either directly or indirectly) shall comply with applicable cybersecurity or information assurance (IA) policies as stated in the DHS Policy Directive 4300A, Information Technology System Security Program, Sensitive Systems, version 13.3, Feb 23, 2023 (hereinafter known as DHS 4300A) and Attachments; DHS National Security Systems Policy Directive 4300B Version 10.1, November 21, 2018 for classified systems (hereinafter known as DHS 4300B); TSA MD 1400.28 Information System Security Program (ISSP); TSA Information System Security Program (ISSP) Policy Directive (PD) and TSA Organizational Defined Parameter (ODP) spreadsheet; supplemental Technical Standards (TSs) and Standard Operating Procedures (SOPs); TSA Cloud Computing Security Handbook (CCSH); the DOD Cloud Computing Security Requirements Guide (CC SRG); and the NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations", Rev 5 standards. This Cybersecurity Policy document serves as a subset to the TSA PD. Additional DHS directives and security related guides for contractors can be found on DHS' security policy site: www.dhs.gov/publication/security-training-contract-policy.

A.3. The Contractor shall comply with Federal, Department of Homeland Security (DHS) and Transportation Security Administration (TSA) security, sensitive information handling, and privacy guidelines in effect at the time of the award of the contract, as well as those requirements that may be added during the contract.

A.4. The Contractor shall perform periodic reviews to ensure compliance with cybersecurity, information security and privacy requirements.

A.5. The Contractor shall comply with proper DHS and TSA security controls to ensure that the Government's security requirements are met. These controls are described in DHS 4300A, TSA MD 1400.28 ISSP, the TSA ISSP PD and TSA ODP security policy documents and is mainly based on the current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 5 standards.

A.6. The Contractor shall include this guidance in all subcontracts at any tier where the subcontractor is performing the work defined in the Statement of Work (SOW), Performance Work Statement (PWS), Statement of Objective (SOO).

A.7. The Contractor shall ensure all its staff members have the required level of approved security clearance commensurate with the sensitivity of the information being accessed, stored, processed, transmitted, or otherwise handled by the system or required to perform the work stipulated by the contract. At a minimum, all Contractor staff shall be subjected to a Public Trust background check and be granted a Public Trust clearance before access to any system or other TSA resources as granted.

A.8. The Contractor shall sign a DHS Form 11000-6 *Non-Disclosure Agreement (NDA)* within thirty (30) calendar days of the contract start date.

A.9. The Contractor shall not release, publish, or disclose agency information to unauthorized personnel, and shall protect such information in accordance with the provisions of pertinent laws, regulations, and policies governing the confidentiality of sensitive information.

A.10. The Contractor shall ensure its staff follow all policies and procedures governing cybersecurity, physical, environmental, and information security described in the various TSA regulations pertaining thereto, and the specifications, directives, and manuals for conducting work to generate the products as required by the contract. Personnel shall be responsible for the physical security of their work area and government furnished equipment (GFE) issued to the contractor under the terms of the contract.

A.11. The Contractor shall make all system information and documentation produced (in support of the contract) available to TSA upon request.

B. Risk Management Framework (RMF):

B.1. The Security Authorization (SA) and Ongoing Authorization (OA) processes, in accordance with recent NIST SP 800-37 Rev 2 (Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy) and SP 800-137 (Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations) are required for all TSA IT systems, including General Support Systems (e.g., standard TSA desktop, general network infrastructure, electronic mail), Major Applications and development systems (if connected to the operational network or processing, storing, or transmitting government data). These processes are documented in the NIST Risk Management Framework (RMF), and the Ongoing Authorization is part of Step 6 "Monitoring" of the RMF. All NIST guidance is publicly available; TSA and DHS security policy is disclosed upon contract award with some exceptions, which are public facing (i.e., DHS Security and Training Requirements for Contractors).

B.2. Data Privacy and Protection: See *SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)* and *INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)* for additional clauses.

a) The contractor shall satisfy requirements to work with and safeguard Controlled Unclassified Information (CUI), which includes Sensitive Security Information (SSI), Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), and others (See Appendix G for other examples). All support personnel shall understand and rigorously follow DHS and TSA requirements, SSI Policies and Procedures Handbook, and Privacy policies, and procedures for safeguarding SSI, PII and SPII.

b) The Contractor shall be responsible for the security of i) all data that is generated by the contractor on behalf of the TSA, ii) TSA data transmitted by the contractor, and iii) TSA data otherwise stored or processed by the contractor regardless of who owns or controls the underlying systems while that data is under the contractor's control. All TSA data, including but not limited to: CUI, PII, SPII, SSI, NSS, and Critical Infrastructure Information (CII) shall be protected according to DHS and TSA security policies and mandates.

c) TSA shall identify IT systems transmitting any classified/unclassified/SSI information and requiring protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:

    a. FIPS 197 (**Advanced Encryption Standard (AES)) 256 algorithm (or higher)** and cryptographic modules that have been validated under FIPS 140-3.
    b. National Security Agency (NSA) Type 2 or Type 1 encryption (current version)
    c. Public Key Infrastructure (PKI) (see current DHS 4300A), key cards, biometrics, or in the case of multi-factor authentication MFA), some combination therein (See Attachment U) Information Security Sensitive Systems Program Directive 4300A v 13.3, Feb 2023.

d) The contractor shall maintain data control according to the TSA security level of the data. Data separation shall include the use of discretionary access control methods, VPN encryption methods, data aggregation controls, data tagging, media marking, backup actions, and data disaster planning and recovery. Contractors handling SPII shall comply with TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information* (current version).

e) Users of TSA IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing TSA IT assets are expected to actively apply the practices specified in the TSA ISSP PD, TSA ODP, and applicable Technical Standards and SOPs.

f) The contractor shall comply with SPII disposition requirements stated in the TSA ISSP PD, applicable Technical Standards, SOPs and TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*.

g) The Contractor shall ensure all source code is protected from unauthorized access, alterations, or dissemination (see TSA ISSP PD, Technical Standard).

B.3. A written Authorization to Operate (ATO) granted by the TSA Authorizing Official (AO) is required prior to processing operational data or connecting to any TSA network. Contractor shall provide all necessary system information in support of the Security Authorization (SA) process. The AO shall ensure all TSA information systems undergo security assessment and authorization and obtain an ATO prior to operation and deployment. This includes all systems (including pilots) that connect to the TSA network or process TSA sensitive data. The AO shall grant a maximum of two Interim Authorizations to Operate (IATOs) for pilot systems and pilot systems shall not be connected to, or deployed as, an operational system until an ATO is issued. ATOs for Pilot systems **shall not exceed ninety (90) days** and these systems shall be removed from the operational network unless an extension is approved by the AO.

B.4. TSA shall assign a security category to each IT system compliant with the requirements of Federal Information Processing Standards (FIPS) Pub 199 *Standards for Security Categorization of Federal Information and Information Systems* impact levels and assign security controls to those systems consistent with FIPS Pub 200 *Minimum Security Requirements for Federal Information and Information Systems* methodology. Additionally, compliance shall be in accordance with (IAW) NIST 800-60 Volume 2 and Volume 1: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.

B.5. Unless the AO specifically states otherwise for an individual system, the duration of any accreditation shall be dependent on the FIPS 199 rating and overall residual risk of the system; the length can span up to 36 months.

B.6. The Security Authorization (SA) Package contains documentation required for SA and Ongoing Authorization (OA). The package shall contain the following security documentation as required by the DHS OA Methodology:

a) Security Assessment Report (SAR)
b) Security Plan (SP)
c) Contingency Plan
d) Contingency Plan Test Results
e) Federal Information Processing Standards (FIPS) 199 Security Categorization
f) Privacy Threshold Analysis (PTA)
g) E-Authentication
h) Security Assessment Plan (SAP)
i) Authorization to Operate (ATO) Letter
j) Plan of Action and Milestone (POA&M)
k) DHS Ongoing Authorization Artifacts

The SA package shall document the specific procedures, training, and accountability measures in place for systems that process Personally Identifiable Information (PII). All security compliance documents shall be reviewed and approved by the CISO and the IAD and accepted by the Contracting Officer (CO) upon creation and after any subsequent changes, before they go into effect. Note: The CO shall not alter or remove any documentation or language once approved by IAD or authorized members of its staff.

Ongoing Authorization artifacts include monthly TRigger Accountability Log (TRAL), monthly operating system scan results, application scans as directed, updated control allocation table (CAT), and associated memos as directed. All steps in the DHS Mandated tool or System of Record shall be completed correctly, thoroughly and in a timely manner for all steps of the RMF.

B.7. The Contractor shall support the successful remediation of all identified system weaknesses and vulnerabilities that are identified as a result of the aforementioned security review process.

B.8. The Contractor shall submit and analyze monthly operating system vulnerability scans for the DHS Information Security Performance Plan FISMA Scorecard. Vulnerabilities not remediated are generated into Plan of Action and Milestone (POA&Ms) after 30 days.

B.9. Training Requirements:

a) All newly-arrived Contractor employees requiring system access shall receive initial cybersecurity training within 60 days of assignment to the contract via the Online Learning Center (OLC); the COR shall initiate and facilitate this access. Refresher training shall be completed annually thereafter via OLC in accordance with FISMA mandated policy to safeguard TSA's mission and assets.

b) The Contractor shall complete any TSA-related Privacy training on an annual basis.

c) Role-Based training is required for contract employees with Significant Security Responsibility (SSR), whose job proficiency is required for overall network security within TSA and shall be in accordance with DHS and TSA policy. The contractor shall be notified if they have a position with Significant Security Responsibilities.

d) Individuals with SSR shall have a documented individual training and education plan, which shall ensure currency with position skill requirements, with the first course to be accomplished within 90 days of employment or change of position. The individual training plan shall be refreshed annually or immediately after a change in the individual's position description requirements.

e) Cybersecurity and privacy training supplied by the Contractor shall meet standards established by NIST and set forth in DHS and TSA security policy.

f) The Contractor shall maintain an accurate and up-to-date list of all vetted contractor employees who have completed training and shall submit this list to the Contracting Officer Representative (COR) upon request, or during DHS/TSA onsite validation visits performed on a periodic basis.

g) The contractor shall ensure its employees review, understand, and sign the TSA Form 1403 *Computer and Wireless Mobile Device Access Agreement (CAA)* prior to accessing any IT systems.

B.10. Configuration Management (hardware/software/applications):

a) Hardware or software configuration changes shall be in accordance with the current DHS Information Security Performance Plan, the DHS Continuous Diagnostics and Mitigation (CDM) Program to include dashboard reporting requirements and TSA's Configuration Management policy. The TSA Chief Information Security Officer (CISO)/Executive Director for Information Assurance and Cybersecurity Division (IAD) shall be informed of and aware of all configuration changes to the TSA IT environment including, but not limited to systems, hardware, software, applications, infrastructure architecture, infrastructure assets, and end user assets. The TSA IAD POC shall approve any Request for Change (RFC) prior to any development activity occurring for that change and shall define the security requirements for the requested change. The COR shall provide access to the DHS Information Security Performance Plan.

b) The Contractor shall ensure all application, software and/or configuration patches and/or Requests for Change (RFC) have approval by the Technical Discussion Forum (TDF), Change Control Board (CCB) and lab regression testing prior to controlled change release under the security policy document, TSA MD 1400.28 ISSP, TSA PD and TSA ODP, unless immediate risk requires immediate intervention.

c) Approval for immediate intervention (i.e., emergency change) requires approval of the TSA CISO, CCB co-chairs, and the appropriate Operations Manager, at a minimum.

d) The Contractor shall ensure all sites, facilities or operational functions impacted by patching are compliant within 14 days of change approval and release.

e) The acquisition of commercial-off-the-shelf (COTS) Information Assurance (IA) and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting "sensitive information") shall be limited to those authorized products that have been carefully analyzed, reviewed, evaluated, and validated, as appropriate, in accordance with the following:

- The NIST FIPS validation program.
- The National Security Agency (NSA)/NIST, National Information Assurance Partnership (NIAP) Evaluation and Validation Program.
- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement.

f) US Government Department of Defense/Department of Homeland Security, Security Technical Implementation Guides (STIGs):

1. The provider of information technology shall certify all applications are fully functional, safe, secure and operate correctly as intended on systems using the US DoD Security Technical Implementation Guides (STIGs) and in accordance with DHS and TSA guidance.

a. DoD STIGs/SRG: https://public.cyber.mil/stigs/

b. DHS Sensitive Systems Configuration Guidance:

The standard installation, operation, maintenance, management, updates and/or patching of software shall not alter the configuration settings from the approved United States Government Configuration Baseline | CSRC (nist.gov) (USGCB) configuration. The information technology shall also use the Windows Installer Service for installation to the default "program files" directory and shall be able to discretely install and uninstall.

2. Applications designed for general end users shall run in the general user context without elevated system administration privileges.

g) The Contractor shall establish processes and procedures for continuous monitoring (ConMon) of Contractor systems that contain TSA data/information by ensuring all such devices are monitored by, and report to, the TSA Security Operations Center (SOC). The Contractor shall perform monthly security scans on servers and other required assets that contain TSA data and shall send monthly scan results to the TSA IAD.

B.11. Contingency Planning:

a) The Contractor shall develop and maintain a Contingency Plan (CP), to include a Continuity of Operation Plan (COOP), to address circumstances whereby normal operations may be disrupted and thus requiring activation of the CP and/or COOP. The contractor's CP/COOP responsibility relates only to the approved system(s) they provide or operate under contract. Additionally, the CP/COOP shall align to a Business Impact Analysis (BIA), which establishes processes for identifying the critical information and services of TSA systems, IT assets, and the resources required to support them.

b) The Contractor shall ensure that contingency plans are consistent with template provided in DHS Mandated System of Record. If access has not been provided initially, the contractor shall use the DHS 4300A, Attachment K *IT Contingency Plan Template*.

c) The Contractor shall identify and train all TSA personnel involved with COOP efforts in the procedures and logistics of the disaster recovery and business continuity plans.

d) The Contractor shall test their CP annually and retain records of the annual CP testing for review during periodic audits.

e) The Contractor shall record, track, and correct any CP deficiency; any deficiency correction that cannot be accomplished within one month of the annual test shall be elevated to IAD management.

f) The Contractor shall have an up-to-date Emergency Response Plan (ERP), Backup Operations Plan (BOP) and a Post-Disaster Recovery Plan (PDRP).

g) The Contractor shall ensure all TSA data (e.g., email servers, data servers, etc.) is incrementally backed up daily.

h) The Contractor shall ensure a full backup of all network data occurs as required by the system's *availability* security categorization impact rating per the TSA ISSP PD.

i) The Contractor shall ensure backup of data to facilitate a full operational recovery within one (1) business day at either the prime operational site or the designated alternate/backup site in accordance with local disaster recovery plan.

j) The Contractor shall ensure that data at the secondary location is current as required by the system's *availability* security categorization impact rating.

B.12. Program Performance and Audit:

a) The Contractor shall comply with requests to be audited and provide responses within three (3) business days to requests for data, information, and analysis from the TSA IAD and management, as directed by the CO. These audits shall include, but are not limited to, requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

b) Upon completion of monthly security scans, findings shall be documented and categorized as High, Moderate, or Low based on their potential impact to the System IT security posture.

c) The Contractor shall afford DHS/TSA access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract.

B.13. Data Stored/Processed at Contractor Site:

a) Unless otherwise directed by TSA, any storage of data shall be contained within approved resources allocated by the Contractor (and approved by TSA) to support TSA and may not be on systems that are shared with other commercial or government entities or clients.

b) The AO shall approve the use of any contractor portable storage media on external systems.

c) The SO shall ensure the approved alternate storage site is physically secured to an equivalency of the primary storage site, using access controls.

B.14. Remote Access:

a) Any TSA-approved Contractor remote access connection to TSA networks shall be considered a privileged arrangement for both Contractor and the Government to conduct

sanctioned TSA business. Therefore, remote access rights shall be expressly granted, in writing, by the TSA AO.

b) Any unauthorized Contractor employee(s) remote access connection to TSA networks shall be terminated immediately at the sole discretion of TSA.

c) The Contractor shall use his or her federally issued and approved personal identity verification (PIV) credential/identification badge to access TSA resources to include IT applications and physical facility.

B.15. Disposition or decommission of Government Resources:

a) At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract and provide signed certifications that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.28 ISSP, TSA ISSP PD, Technical Standards and SOPs. The contractor shall certify in writing that sanitization or destruction has been performed. Sanitization and destruction methods are outlined in the NIST Special Publication 800-88 Guidelines for Media Sanitization, TSA Technical Standard 046 *IT Media Sanitization and Disposition*, and SOP 1400-503 *IT Media Sanitization*. The contractor shall email TSA, PM, CO, and COR a signed certification by the contractor's designated senior security officer or senior official, signed proof of sanitization. In addition, the contractor shall provide the TSA CO a master asset inventory list that reflects all assets, government furnished equipment (GFE) or authorized non-GFE that were used to process and store TSA information.

B.16. Software Guidance:

The CO shall provide a listing of all TSA approved security software upon contract award. The approved security software listing is maintained by the IAD.

a) In support of the CDM objective to protect high value assets (HVAs) and information, the TSA has acquired security tools to conduct Indicator of Compromise (IOC) scans within the mandated time frame. The Government shall provide the tool license and/or equipment for installation of tool agents on all TSA supported assets.

b) The contractor shall support efforts to allow for the IOC scanning mandate. This may include installation of tool servers and/or agents within each system's environment and on all TSA supported assets. The Government shall provide the contractor with the tool server(s) that shall not belong to the contractor's system boundary. The tool server shall be reachable from OneNet/TSANet over the Internet. The tool server(s) shall be properly configured to reach all assets with the tool agent installed on the network. Credentials (service accounts) shall be provided for IOC scans and tool interrogation.

c) The contractor shall support or perform the installation of forensic software servlet agents on supported Operating Systems on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards. The contractor shall test and

upgrade the servlet agents as directed by the IAD.

d) The Government shall provide the contractor with a forensic software server that shall not belong to the contractor's system boundary. The contractor shall support or perform the installation of the server. The server shall be reachable from TSANet over the Internet and shall be primarily used for authentication and proxy functions. The server shall be properly configured to reach all assets with the agent installed on the network.

e) The contractor shall support efforts of incident response and forensic investigation. This includes authorization to connect TSA authorized equipment where the forensic software servlet agents are reachable to perform analysis.

f) The contractor shall install TSA-provided solution patches within two (2) days of issuance, or as directed by TSA CIO, and provide evidence of implementation to the TSA ISSO.

g) End-of-Life (EOL) / End-of-Service (EOS):

1) The Contractor shall ensure that any hardware, software, or application that is procured develops a full lifecycle plan based on the vendor's established life and service expectancy of the product and total cost of ownership. Any new or existing product that shall reach end-of-life (EOL)* within three (3) years and is part of a TSA FISMA IT System shall require development of a remediation, upgrade, replacement, and funding plan to remove the EOL item(s) from the TSA environment completely within that time frame. A plan of action and milestone (POA&M) shall be submitted for risk acceptance to the TSA CISO to track remediation milestones appropriately.

*EOL / EOS - Defined as production and/or development, technical support, application updates, spare parts and security patches which are no longer available from the vendor.

B.17. Maintenance:

a) The Contractor shall ensure that the system, once operational, is properly and securely maintained and monitored, to include immediate response to critical security patches, routine maintenance windows to allow for system updates, and compliance with a defined configuration management process. All patches and system updates shall be properly tested and approved in a development environment ***before*** being implemented in the production environment.

b) The contractor shall perform customer support twenty-four (24) hours, seven (7) days a week (i.e., 24/7) within the Continental United States (i.e., CONUS) only.

C. *Continuous Diagnostics and Mitigation:*

C1. The Government, through a Continuous Monitoring as a Service (CMaaS) vendor, shall provide the contractor with GFE appliances and tools to support the implementation and maintenance of the Continuous Diagnostics and Mitigation (CDM) Solution. The tools shall be hosted on the DHS' Infrastructure as a Service (IaaS) program. The Government, through the CMaaS vendor, shall provide sensor kits, appliances, probes, and agents that shall be deployed on all contractor Information Systems supporting the TSA.

C2. The contractor shall support the installation (including rack and configuration) of sensor kits, appliances, probes, and agents on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards.

C3. The contractor shall configure/tune their existing endpoint security products to coexist with the identified products to ensure smooth and cohesive functionalities. Credentials (service accounts) shall be provided by the TSA CISO, or designee, for vulnerability scans and host interrogation.

C4. The Government, through the CMaaS vendor, shall provide the following support for operations and maintenance of the CDM solution sensor kits:

a) Patching (Controlled through a CMaaS Windows Server Update Service (WSUS))
b) Hardware troubleshooting & Risk Management (RMA)
c) Application maintenance (done from the Government/TSA Management Enclave)
d) Vulnerability scanning

C5. The contractor shall install TSA-provided CDM Solution patches within two (2) days of issuance, or as directed by TSA, and provide evidence of implementation to the TSA ISSO.

C6. The TSA CO (as approved and on behalf of the SO and TSA senior leadership) is authorized to provide technical direction to the contractor for the sole purpose of implementing the CDM Solution. If the technical direction results in any cost incurred by the contractor, for which the contractor shall seek reimbursement from the Government, the contractor shall identify the following information in any cost/price proposal to the Government: name of system owner, summary of the technical direction, date of the technical direction, purpose of the technical direction, summary of actions taken by the contractor, any other information the CO may require to further guide the directed change. The contactor shall receive approval from the CO of the directed and approved change prior to incurring costs associated with the technical direction.

C7. Personal Identity Verification (PIV) and Login:

a) The Contractor shall use PIV credential/identification badges as the primary means to access TSA resources to include IT applications and physical facility. TSA network domain user account password expiration function shall be disabled when using PIV Machine Based Enforcement (MBE). PINs for PIV card-enabled users shall not expire and shall have a minimum six-digit PIN when logging into the network using a PIV card.

b) The Contractor shall ensure newly developed information system(s) support PIV card authentication. The information system shall be capable to accept and electronically verify PIV credentials.

c) The Contractor shall employ information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

d) The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the approved PIV credentials as the common means of authentication for access to DHS/TSA facilities, networks, and information systems. PIV credentials shall be used as the primary means of authentication for DHS/TSA sensitive IT systems. The Contractor shall use his or her federal issued PIV credentials to access TSA resources to include IT applications and physical facility.

e) The DHS/TSA Security Office shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued PIV credentials/identification cards and building passes that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or any other TSA-issued cards.

f) The contract ISSO shall determine and enforce the appropriate frequency for changing passwords/PINs in accordance with appropriate guidance documentation along with the use of a second factor authentication to follow Executive Order 14028 "Improving the Nation's Cybersecurity" for Multi-factor Authentication (MFA). In the absence of specific guidance, where applicable, passwords shall not remain in effect longer than ninety (90) days.

D. Federal Risk and Authorization Management Program (FedRAMP):

D1. If a vendor is to host a system with an approved Cloud Service Provider (CSP), the CSP and shall adhere to the following:

a) Comply with Federal Agency cloud requirements per CCSH;

b) Identity and entitlement access management shall be done through Federated Identity;

c) SSI, PII and SPII shall be encrypted in storage and in transit as it is dispersed across the cloud;

d) Sanitization of all TSA data shall be done as necessary at the IaaS, PaaS, or SaaS levels;

e) Cloud bursting shall not occur;

f) TSA data shall be logically separated from other cloud tenants;

g) All system administrators shall be properly cleared and vetted U.S. citizens;

h) TSA data shall not leave the United States; and

i) The cloud internet connection shall route via an approved DHS Trusted Internet Connection (TIC) and intrusion detection system (IDS). These include but are not limited to the analysis of network flow records, detecting, and alerting to known or suspected cyber threats, intrusion prevention capabilities and under the direction of DHS detecting and blocking known or suspected cyber threats using indicators. The IDS capability shall use the Domain Name Server Sinkholing capability and email filtering capability allowing scans to occur destined for .gov networks with malicious attachments, Uniform Resource Locators, and other forms of malware before being delivered to *.gov end-users.

D2. Private Sector System Requirements: TSA shall conduct audits at any time on approved private sector systems, and the system shall be entered into the TSA FISMA Inventory as a system of record (SOR) using the Control Implementation Summary (CIS) provided by the Cloud Service Provider. Security artifacts shall be created and maintained in the DHS Mandated System of Record. The private sector systems are required to go through the Security Authorization Process and the RMF in accordance the Federal Information Systems Management Act (FISMA) and NIST SP 800-37. The cloud internet connection shall be behind a commercial Trusted Internet Connection (TIC) that has an approved IDS deployed. Security event logs and application logs shall be sent to the TSA SOC. Incidents as defined in the TSA MD 1400.28 ISSP, and its Attachment 1 (TSA ISSP PD and TSA ODP) shall be reported to the TSA SPOC 1-800-253-8571. DHS Information Security Vulnerability Management Alerts and Bulletins shall be patched within the required time frames as dictated by DHS and communicated by the COR or contract security point of contact (POC).

E. Interconnection Security Agreement (where applicable):

If the service being supplied requires a connection to an outside non-DHS/non-TSA Contractor system, or DHS system of different sensitivity, the following shall apply:

E1. Interconnections between DHS/TSA and non-DHS/TSA IT systems (i.e., Contractor Owned Contractor Operated (COCO) systems) shall be established only through authorized contractual agreements and funding, controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information security on the network. Connections with other Federal agencies shall be documented using an approved Interagency Agreements (IAA); Memoranda of Understanding/Agreement (MOU/MOA), Service Level Agreements (SLA) or Interconnection Service Agreements (ISA).

E2. ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.

E3. ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.

1.3 ITAR SME Cybersecurity Supply Chain Risk Management (C-SCRM)

Cybersecurity C-SCRM language is applicable for requirements for the use of supplies and services to include the following:

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:

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.

1.4 DHS and TSA Enterprise Architecture (August 2025):

a) The Contractor shall ensure that all architectural artifacts including but not limited to solutions, business processes, data, IT elements for legacy Transportation Security Equipment (TSE), Information Systems Security Agreements (ISSAs), System Design Documents (SDDs), deliverables, and services, are aligned and compliant with the current DHS and TSA Enterprise Architecture (EA), and The Common Approach to Federal Enterprise Architecture, the Technology Business Management (TBM) Taxonomy, and the Federal Information Technology Acquisition Reform Act (FITARA).

i. All solutions and services shall comply with DHS and TSA Enterprise Architecture policies, standards, and procedures. Specifically:

a. DHS and TSA Enterprise Architecture policies, standards, and procedures.
b. Homeland Security Enterprise Architecture (HLS EA) and TSA EA requirements.
c. TSA and DHS IT Security and Cloud Architecture.
d. Infrastructure Architecture, including Network, Conceptual Network Diagram (CDM), and Logical Network Diagram (LDM).
e. Application/Systems Architecture, including System Design Document (SDD), System Security Plan (SSP), Interface Control Documents (ICD), Entity Relationship Diagram (ERD), and Tech Stack /Tech Stack Open Source.
f. Information/Data Architecture.
g. Performance Architecture, including Key Performance Parameters (KPP's).
h. Business Architecture policies, directives, guidelines, standards, Concept of Operations (CONOPS), segment architectures, and reference architectures.
i. TSA functional capabilities.
j. TSA operational capabilities.
k. TSA lines of business.
l. TSA business process flows (As-Is and To-Be).
m. TSA funding sources.
n. TBM Taxonomy for IT cost transparency.

ii. All software and tools used to build, develop, or deploy IT solutions for TSA shall leverage the TSA NextGen Architecture (NGA) Technology Stack, known as "The Kit". In accordance with TSA CIO Priority 2.1 "Modernize, Simplify, Reduce, and Enforce

TSA IT and Data Toolkit", the use of "the Kit" will drive modernization and simplification, with the goal of reducing the current TSA Technology Footprint.

iii. This includes both the new Transportation Security Equipment (TSE) and legacy TSE that utilizes IT software, services, or equipment including embedded IT elements such as network switches, routers, printers, etc.

iv. All solutions shall implement and leverage TSA Information and Data Standards as defined and approved by TSA policy.

v. All solution architectures and services (e.g., Application, System, Network, Security, Information/Data, Cloud) shall be reviewed and approved by TSA EA as part of the TSA System Engineering Life Cycle (SELC) review process, in accordance with TSA IT Governance Management Directive 1400.20 and applicable DHS and TSA IT governance policies, directives, and processes. This includes the Solution Engineering Review (SER), Preliminary Design Review (PDR) and Critical Design Review (CDR) stage gates.

The required design artifacts include solution approach document, the PDR document, and the System Design Document (SDDs) as directed by A&DMB. Successful completion of the PDR/CDR stages results in an approved architecture, which is required before proceeding to development. An approved architecture is also a necessary critical step in obtaining an Authority to Operate (ATO).

All implementations shall adhere to the approved solution architecture/design without deviation. Any changes to the previously approved solution and/or design identified during subsequent SELC phases - including testing, implementation, and deployment - shall undergo additional EA review before proceeding.

vi. TSA Offices acquiring enterprise architecture services at the segment or solution level shall engage and collaborate with the TSA Architecture and Data Management (A&DM) Branch to ensure strategic alignment of people, processes, information, and technology, while complying with enterprise-level architecture governance, artifacts, and standards.

a. The Contractor shall engage domain architect(s) in A&DM prior to the SELC Obtain Phase, i.e. during the SELC Need or "Analyze and Select" Phase.
b. The Contractors shall collaborate with the EA domain architect(s) to deliver the required design artifacts and achieve the desired outcome under their guidance.
c. The Contractor shall provide architecture and system/application data and models in prescribed formats for storage in TSA's Enterprise Architecture Repository.

b) In accordance with the TSA Cloud Strategy 2.0, (April 2019), TSA's approach to cloud computing and governance of migration to the cloud requires the Contractor to ensure that

cloud solutions primarily utilize the SaaS (Software as a Service) model for implementation. When necessary, the Contractor may also use Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). The Contractor shall adhere to the principles outlined in the cloud strategy to systematically retire or replace legacy applications through an integrated approach to cloud planning, architecture, hybrid deployment, and operation.

c) The applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) for individual acquisitions shall comply with the DHS Enterprise Architecture, as outlined in OMB Memorandum M-21-07 (November 2020), regardless of whether the acquisition involves modification, upgrade, or replacement. All EA related component acquisitions must be IPv6 compliant, as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Information and Data Governance and Management

d) The Contractor shall develop, use, and dispose of TSA information and data assets in accordance with TSA governance processes established by the Enterprise Information/Data Governance Board (EIDGB) and in compliance with the DHS Enterprise Data Governance and Management Directive (MD) 103-01.

i. TSA information and data assets include but are not limited to the TSA Data Catalog, TSA Information and Data Standards, TSA Data Management Plan, TSA data sets (including open data sets for public consumption), TSA information and data stored in TSA repositories, TSA information and data in systems and applications (internal and external), and TSA information exchanges.

ii. All TSA information and data, as well as all solutions that capture, store, use, and provide TSA information and data, shall comply with the Geospatial Data Act (GDA) of 2018 (P.L. 115-254). This act requires agencies to foster efficient management of geospatial data/information, technologies, and infrastructure through enhanced coordination among Federal, state, local, and tribal governments, as well as private sector and academia.

iii. Description information for all data assets shall be submitted to the TSA Enterprise Architecture Team, which will be responsible for coordination with DHS, as well as for review, approval and insertion into the TSA Data Reference Model and Enterprise Architecture Repository.

iv. In addition to the Federal Acquisitions Regulations (FAR) Subpart 27.4 - 'Rights in Data and Copyrights' and Section 35.011 detailing technical data delivery, the Contractor shall provide all TSA-specific data in a format that maintains pre-existing

referential integrity and data constraints, as well as data structures in a format understandable to TSA. Examples of data structures include, but are not limited to:

a. Data models containing entities and attributes, identifying authoritative and trusted data sources, and depicting relationship mapping and/or linkages.
b. Metadata information to define data definitions.
c. Detailed data formats, types, and sizes.
d. Delineations of referential integrity (e.g., primary key/foreign key) of data schemas, structures, and/or taxonomies.
e. Information exchange specifications.

v. All TSA-specific data shall be delivered to TSA in a secure and timely manner. Data security is defined within the "Requirements for Handling Sensitive, Classified, and/or Proprietary Information" section of this Statement of Work (SOW), Statement of Objectives (SOO), and Performance Work Statement (PWS). This definition applies not only to the delivery of data but also to maintaining TSA-specific data within a non-TSA or DHS proprietary system.

vi. All metadata shall be pre-defined upon delivery to TSA. Metadata shall be delivered in a format that is readily interpretable by TSA (e.g., metadata shall be extracted from any metadata repository not utilized by TSA and delivered in a TSA approved manner). Metadata shall also include an indication of historical versions, the most current data to be used, and the frequency of data refreshes.

vii. The Contractor shall provide a Data Asset Repository Profile (DAR) and Data Management Plan (DMP) to EA team using EA-provided template prior to the preliminary/critical design review. The DAR and DMP shall include conceptual and logical data models, data dictionaries, data asset profile, and other artifacts pertinent to the project's data.

viii. TSA adheres to the DHS National Information Exchange Model (NIEM) First policy and standards, as outlined in the DHS Memorandum, "Adoption of the National Information Exchange Model within the Department of Homeland Security," dated May 3, 2019. All TSA information and data exchanges shall be NIEM compliant. Additionally, all TSA solutions that leverage TSA information and data exchanges shall be NIEM compliant.

1.5 ITAR SME FedRAMP – Cloud and 'as-a-Service'

(a) 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:

i. 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.
ii. 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.
iii. 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).

1.6 ITAR SME Geospatial DATA ACT (GDA)

In accordance with the Geospatial Data Act (GDA) of 2018 (U.S. Code, Title 43 – Public Lands, Chapter 46: Geospatial Data) all vendors shall:

- Ensure that all geospatial data, created or procured, complies with, Federal Geographic Data Committee (FGDC) endorsed standards and Department of Homeland Security Geospatial Management Office policies and best practices for metadata, records retention and privacy requirements.

- Ensure interoperability of geospatial data and allocate resources for effective data management.

- Support DHS in reducing duplicative data acquisition, as appropriate, by searching available data at Data.gov, Sam.gov and data from Homeland Security Enterprise partners (including, state, local, Tribal governments, private sector, and academia).

- Ensure that geospatial data is made available to the public, as appropriate

1.7 ITAR SME Identity and Credentials Management (ICAM)

HSPD-12:

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to DHS facilities, networks, and information systems. Personal Identity Verification (PIV) credentials shall be used as the primary means of logical authentication for DHS sensitive systems. The Contractor must use his or her federal issued Personal Identity Verification (PIV) credentials to access DHS resources to include IT applications and physical facility.

The DHS Office of the Chief Security Officer shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer's Representative (COR) all DHS issued Personal Identity Verification (PIV) credentials /identification cards and building passes that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or card. The Contractor or contractor personnel's failure to return all DHS issued identification cards and building passes upon expiration, upon the contractor personnel's removal from the contract, or upon demand by DHS may subject the contractor personnel and the Contractor to civil and criminal liability.

1.8 ITAR SME Privacy

- *FAR 52.224-3 Privacy Training – Alternate I (DEVIATION) (see FAR Class Deviation 17-03, Revision 1) (July 2023)*
- *3052.204-71 Contractor Employee Access (July 2023)*
- *HSAR 3052.204-72 Safeguarding Controlled Unclassified Information (July 2023)*
- *HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents (July 2023)*
- *Special Clause Information Technology Security Awareness Training (July 2023) (see HSAR Class Deviation 15-01, Revision 1)*

FAR 52.224-3 Privacy Training – Alternate I (DEVIATION 17-03) (July 2023)

(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.

(End of clause)

ALTERNATE I (JULY 2023)

(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:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
(2) 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.

ALTERNATE II (JULY 2023)

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

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

3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JULY 2023)

(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 3052.204-72 Safeguarding of Controlled Unclassified Information (July 2023):

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

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

(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 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);
(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 3052.204-72 Safeguarding of Controlled Unclassified Information - Alternate 1 (July 2023):

(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.

HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents (July 2023):

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

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

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

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

(3) Other PII that may present an increased risk of 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.

Special Clause Information Technology Security Awareness Training (July 2023) (see HSAR Class Deviation 15-01, Revision 1):

(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.

(End of clause)

1.9 Sensitive Security Information (SSI) Training

Contractors are required to complete the TSA Security Fundamentals training course in OLC within the first 60 days to satisfy initial SSI Training. Training will be required to be completed on an annual basis.

[End of ITAR Terms and Conditions]