DEPARTMENT OF HOMELAND SECURITY
OFFICE OF PROCUREMENT OPERATIONS
REQUIREMENTS TOOL

THIS IS A REQUEST FOR INFORMATION (RFI) ONLY

This RFI is issued solely for information and planning purposes and does not constitute a solicitation. Nonetheless, submitters should properly mark their responses if the information is confidential or proprietary. Furthermore, those who respond to this RFI should not anticipate feedback with regards to its submission other than acknowledgment of receipt, should the submitter request an acknowledgement. In accordance with FAR 15.201(e), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. All submissions become the property of the Federal Government and will not be returned. Responders are solely responsible for all expense associated with responding to this RFI.

INTRODUCTION

The Office of Biometric Identity Management (OBIM) provides biometric match, store, share, and analyze services to DHS and mission partners. The need for biometrics continues to grow among DHS Components; interagency stakeholders (e.g., the Departments of State, Justice, and Defense); State, local, tribal, and territorial entities; the Intelligence Community; and international mission partners. Biometrics support critical national security priorities, including counterterrorism and immigration. OBIM is focused on delivering accurate, timely, and high assurance biometric identity information and analysis. OBIM's overall goals and priorities include continuing to improve biometric services and access to expanded biometric data to enable DHS operational missions.

PURPOSE OF RFI

The purpose of this RFI is to gather information on requirements development and management tools available that can capture, develop, store, and assess requirements. The capability will also provide a means to obtain organizational and stakeholder approval of requirements and associated artifacts (e.g., supporting documentation). The tool will also enable the automated generation of use cases, user stories, and test cases.

SUBMISSION REQUIREMENTS

This acquisition is in line with on-going efforts tied to a new OBIM-wide process for managing the requirements (acquisition-based, missional, operational, functional, non-functional, etc.) for OBIM systems and operations referred to as the Requirements Development and Management Process (RDMP), currently on-track for implementation at the start of Q1FY2024, with an eye towards mitigating and resolving identified issues in the current usage of multiple uncoordinated tools for managing requirements. This tool shall meet the following technical criteria:

Functional Criteria

1. The tool must be able to define, manage, and engineer requirements processes.
2. The tool shall serve as a centralized collaboration of the in-house Requirements Development and Management Process platform between multiple and distributed stakeholders.
3. The tool shall be able to score requirements to determine requirements quality, maturity, time to generate, traceability, changes, and validation (among other potential metrics), and provides the data (for a separate analytic environment) and/or a dashboard with the status of the metrics.
4. The tool shall have the capability to know the difference between an operational, non-functional/functional/system/technical requirement based on a maturity of the requirement.
5. The tool shall be able to allow for a review and approval process, requirement reuse, and the support of bug tracking.
6. The tool shall have Full/Read-Write, Read/Only product as such to review requirements, develop, test or design documents that will allow teams to collaborate.
7. The tool shall have documentation and project baselines can be sent out to users for electronic signature and feedback collected in a centralized way, making sure that approved documents are available to everybody in the project.
8. The tool shall have change management: ability to manage the approval of and changes to requirements artifacts within the tool.
9. The tool shall manage Artifact Repository: Artifacts are stored in version-controlled repository that supports check out, update, check-in, and collaboration across multiple types and workspaces.
10. Agile work management: The tool will allow for the automated generation of use cases, user stories, test cases/plans and prioritization.
11. The tool shall facilitate the decomposition of high-level capability requirements into epics, user stories, and features.
12. The tool shall provide the status of requirements, to include but not limited to draft, proposed, approved, scheduled for release, partially implemented, completely implemented, obsolete, cancelled/deleted, etc.
13. The tool shall have ease to interoperate or integrate effectively with any type of process template such as the current suite of Microsoft products and exportable as a .pdf, such as the Microsoft Office 365 versions of Word, Excel, PowerPoint, Visio, and Outlook. This includes compatibility with the Cameo MagicDraw application (or similar architecture and data management tool).
14. The tool shall have ease to integrate effectively and easily with issue tracking and collaboration tools such as the current suite of OBIM agile-supporting requirements tools: JIRA v8.20.1, and Maestro Confluence 7.13.2.
15. The tool shall offer a full array of reporting, cross-referencing, searching, and traceability capabilities for the managed requirements.

Technical Criteria

1. The tool shall support/reside on Amazon Web Services without a bridge product.
2. The tool shall be customizable for flexibility in building reports and/or adding additional features.
3. The tool shall have traceability to the source code with a collaborative role-based sign-off approach for requirements.
4. Technical support for Data base transfer within the tool
5. Vendor availability, support, and quality training: ability to receive timely and support, additional training material required for end users, including videos, user manuals or interactive tutorials.

Software maintenance agreements must be compatible with software purchased. The software license use and maintenance support agreements come with the purchase of a license. Total of 30 licenses with read-write access.

In addition to the requested information above, confirm if the solution described is commercially available or is a commercially available solution that can be modified to meet the Government's needs.

Finally, provide any pricing considerations of which the Government should be aware. For example, does this solution require an initial investment followed by reduced operations and maintenance costs, or is license pricing tier-based with additional discounts available for a higher number of users, etc. Please note that specific pricing for the product **IS NOT** being requested.

SUBMISSION INSTRUCTIONS

The information obtained may be utilized in the preparation of a Request for Quote (RFQ) provided DHS finds it in its best interest. Vendors are encouraged to review this RFI and determine if their competency meet the DHS requirements.

Finally, RFI submissions should include a cover letter no longer than two (2) pages in length with the following information:

1. Vendor official name, address and phone number.
2. Point of Contact information, including name, phone number and email address.
3. The vendor's country of origin.
4. If applicable, one URL for the organization's official web site.
5. The socio-economic category under which the vendor is currently certified to perform under NAICS code [541512 – Computer Systems Design Services].
6. If applicable, your company's GSA Schedule contract number; and
7. If applicable, any relevant DHS strategic sourcing vehicle your company currently holds a contract under and the associated contract number.

Responses are limited to **10 pages** (including cover letter), must be in 12pt Calibri font with .75 inch margins and submitted via e-mail only to Contracting Officer Amy Driver at Amy.Driver@hq.dhs.gov, and Contract Specialist Robert Farrell at Robert.Farrell@hq.dhs.gov no later than May 19, 2023 at 5:00 PM ET. The subject line of the email should contain the RFI number 70RDAD23RFI000014. Proprietary information, if any, should be minimized and MUST BE CLEARLY MARKED. To aid the Government, please segregate and mark proprietary information. Please be advised that all submissions become Government property and will not be returned.

(End of Request for Information)

DEPARTMENT OF HOMELAND SECURITY
OFFICE OF BIOMETRIC IDENTITY MANAGEMENT
STATEMENT OF WORK FOR
REQUIREMENTS MANAGEMENT TOOL

May 2023

1.0 GENERAL

1.1 BACKGROUND

As a program within the U.S. Department of Homeland Security (DHS), the Office of Biometric Identity Management (OBIM) supports DHS' mission to protect our nation by providing biometric identification services to federal, state, and local government decision makers to help them accurately identify the people they encounter and determine whether those people pose a risk to the United States. OBIM's most visible service is the collection of biometrics—digital fingerprints and a photograph—from international travelers at United States visa-issuing posts and ports of entry. Collecting this information helps immigration officers determine whether a person is eligible to receive a visa or enter the United States. The biometric collection process is simple, convenient and secure.

1.2 SCOPE

The scope of this effort is to provide a requirements development and management tool to support the capture and development of functional requirements. The desired capability will provide a means to author and elicit requirements; trace requirements; assess requirement; and obtain organizational and stakeholder approval of requirements. The tool will also allow for the automated generation of use cases, user stories, and test cases. The tool will also be used to support the development of system/technical requirements based on a mature functional requirement.

1.3 OBJECTIVE

OBIM provides a variety of services and information to DHS and other Federal agencies. To accomplish the core Program Missions, OBIM relies on information technology (IT) assets. The objective is for OBIM to obtain a requirements development and management tool (software) to ensure that staff members can fulfill mission obligations.

1.4 APPLICABLE DOCUMENTS

1.4.1 Compliance Documents

- N/A

1.4.2 Reference Documents

- N/A

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 TASK 1: REQUIREMENTS DEVELOPMENT AND MANAGEMENT TOOL

This acquisition is in line with on-going efforts tied to a new OBIM-wide process for managing the requirements (acquisition-based, missional, operational, functional, non-functional, etc.) for OBIM systems and operations referred to as the Requirements Development and Management Process (RDMP), currently on-track for implementation at the start of Q1FY2024, with an eye towards mitigating and resolving identified issues in the current usage of multiple uncoordinated tools for managing requirements. This tool shall meet the following technical criteria:

- Primarily a requirements development and management tool to support the capture and development of functional and non-functional requirements. The desired capability shall provide a means to author and elicit requirements; trace requirements; assess requirements; and obtain organizational and stakeholder approval of requirements.
- The tool shall allow for the automated generation of use cases, user stories, and test cases/plans.
- The tool shall facilitate the decomposition of high-level requirements artifacts into epics, capabilities, and features.
- The tool shall be used to support the development of system/technical requirements based on a mature functional requirement.
- The tool shall support versioning of requirements.
- The tool shall support the status of requirements, to include but not limited to draft, proposed, approved, scheduled for release, partially implemented, completely implemented, obsolete, cancelled/deleted, etc.
- The tool shall integrate effectively and easily with the current suite of Microsoft products, such as the Microsoft Office 365 versions of Word, Excel, PowerPoint, Visio, and Outlook. This includes compatibility with the Cameo MagicDraw application (or similar architecture and data management tool).
- The tool shall integrate effectively and easily with the current suite of OBIM agile-supporting requirements tools: JIRA v8.20.1, and Maestro Confluence 7.13.2.
- The tool shall offer a full array of reporting, cross-referencing, searching, and traceability capabilities for the managed requirements.
- Software maintenance agreements shall be compatible with software purchased. The software license uses and maintenance support agreements come with the purchase of a license. A total of 30 licenses is required with read-write access within 15 calendar days from date of award.
- The tool must be able to define, manage, and engineer requirements processes.
- The tool shall serve as a centralized collaboration of the in-house Requirements Development and Management Process platform between multiple and distributed stakeholders.
- The tool shall be able to score requirements to determine requirements quality, maturity, time to generate, traceability, changes, and validation (among other potential metrics), and provides the data (for a separate analytic environment) and/or a dashboard with the status of the metrics.

- The tool shall have the capability to know the difference between an operational, non-functional/functional/system/technical requirement based on a maturity of the requirement.
- The tool shall be able to allow for a review and approval process, requirement reuse, and the support of bug tracking.
- The tool shall have Full/Read-Write, Read/Only product as such to review requirements, develop, test or design documents that will allow teams to collaborate.
- The tool shall have documentation and project baselines can be sent out to users for electronic signature and feedback collected in a centralized way, making sure that approved documents are available to everybody in the project.
- The tool shall have change Management: Ability to manage the approval of and changes to requirements artifacts within the tool.
- The tool shall managed Artifact Repository: Artifacts are stored in version-controlled repository that supports check out, update, check-in, and collaboration across multiple types and workspaces.
- The tool shall provide the status of requirements, to include but not limited to draft, proposed, approved, scheduled for release, partially implemented, completely implemented, obsolete, cancelled/deleted, etc.
- The tool shall support/reside on Amazon Web Services without a bridge product.
- The tool shall be customizable for flexibility in building reports and/or adding additional features
- The tool shall have traceability to the source code with a collaborative role-based sign-off approach for requirements
- Technical support for Data base transfer within the tool
- Vendor availability, support, and quality training: ability to receive timely and support, additional training material required for end users, including videos, user manuals or interactive tutorials.

2.2 TASK 2: TRAINING

- This procurement is software only and does not require any full-time on-site or off-site contractor staff. Training for the software shall either be virtual or in person instructor led. Instructors shall not have access to any Personally Identifiable Information (PII) on the system.
- The contractor shall provide 10 days single-day classes of real-time instructor-led (either in-person or virtual) professional services training compatible with software purchased.
- The contractor shall provide three (3) days of single-day classes of real-time instructor-led (either in-person or virtual) for Jira synchronization training, configuration, and sync bridge.

2.3 TASK 3: CUSTOMER SUPPORT

- Telephone and/or email support to include customer portal account/access for the duration of the period of performance shall be provided between 8am to 5pm EST/EDT Monday – Friday.

2.4: TASK 4: MAINTENANCE AND UPDATES

- Maintenance and updates shall be required on an as-needed basis. All updates shall be completed after 5pm or before 8am EST/EDT in order not to interrupt account accessibility.

3. PLACE OF PERFORMANCE

The place of performance will be at the OBIM office located in the National Capital Region (NCR).

4. PERIOD OF PERFORMANCE

The period of performance for this acquisition is one (1) 12-month base period and four (4) 12-month option periods.

5. TRAVEL

Contractor travel shall not be required for this requirement.

6. POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer, COR, and TM no later than ten (10) business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract. The Post Award Conference will be held at the Government's facility, located at the OBIM offices at 1616 N Ft Myer Drive, Arlington, VA 22209 or via teleconference.

7. OPTION TO EXTEND THE TERM OF THE CONTRACT

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of task order expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the task order expires. The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.
(End of Clause)

8. DELIVERABLES

The contractor shall deliver all required software in accordance with Federal procurement guidelines and agreements. The license key delivery information will be provided at award.

The following table identifies the required deliverable's format and due date(s) for submission.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	6	Post Award Conference	10 calendar days after date of award	N/A
2	4.8	30 Licenses with Read-Write Access	Within 15 calendar days of date of award	TM
3	2.2	10 Day Long Trainings	Within 20 calendar days of award	OBIM personnel
4	2.2	3 Day Long Trainings	Within 20 calendar days of award	OBIM personnel

Upon receipt of the software package, license keys, and documentation deliverables, the Technical Manager (TM) and Contracting Officer's Representatives (CORs) will have 15 calendar days for final review prior to acceptance or providing documented reasons for non-acceptance. If the government fails to complete the review within the review period, the deliverable will become accepted by default. In the event of a rejected deliverable, the contractor will be notified in writing by a COR of the specific reasons for rejection.

For the delivery of training, within 20 calendar days of award or execution of a modification to exercise an option for training, the contractor shall coordinate with the TM to establish a specific date and time for the training.

9. COMPLIANCE TERMS AND CONDITIONS

9.1 DHS ENTERPRISE ARCHITECTURE COMPLIANCE TERMS AND CONDITIONS

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:
- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (1Pv6) to DRS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related

component acquisitions shall be IPv6 compliant as defined in the US. 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."

9.2 Section 508

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendix A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

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

Section 508 Requirements for Technology Products (include in the SOW, PWS, or SOO).

Section 508 applicability to Information and Communications Technology (ICT): ACTIVENAV File Analysis Software Licenses.

Applicable Exception: N/A   Authorization #: N/A.

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components (including but not limited to Other): Does not apply.

Applicable 508 requirements for software features and components (including but not limited to electronic content and software authoring tools and platforms).

Applicable 508 requirements for hardware features and components: Does not apply.

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply.

Section 508 Deliverables (include in the SOW, PWS, or SOO).

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

9.3 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-

296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.
"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:
(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)
Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.
(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:
(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Policy Directive 4300A

(3) DHS Security Authorization Process Guide
(4) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(5) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(6) DHS Information Security Performance Plan (current fiscal year)
(7) DHS Privacy Incident Handling Guidance
(8) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(9) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(10) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html
(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.
(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Policy Directive 4300A* provides the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.
(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.
(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.
(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Policy Directive 4300A* (Version 13.3, February 13, 2023) or any successor publication, and the *Security Authorization Process Guide* including templates.

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

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

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

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for

acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

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

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

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

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

(f) *Sensitive Information Incident Reporting Requirements.*

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

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

(i) Data Universal Numbering System (DUNS).

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime contractor location.

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email).

(v) Contracting Officer POC (address, telephone, email).

(vi) Contract clearance level.

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network.

(viii) Government programs, platforms or systems involved.

(ix) Location(s) of incident.

(x) Date and time the incident was discovered.

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level.

(xii) Description of the Government PII and/or SPII contained within the system.

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

(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

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

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

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

(i) Inspections,
(ii) Investigations,
(iii) Forensic reviews, and
(iv) Data analyses and processing.

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

(h) *Additional PII and/or SPII Notification Requirements*.
(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.
(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

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

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:
(1) Provide notification to affected individuals as described above; and/or
(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company

with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

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

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

(i) A dedicated telephone number to contact customer service within a fixed period.
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores.
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics.
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate.
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

9.4 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

(b) *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.
(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

9.5 OCIO CISO CYBER-SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

a. The Offeror understands and agrees that the Government retains the right to cancel or terminate the Contract, if the Government determines that continuing this solicitation presents an unacceptable risk to national security.

b. “Gray-Market” Equipment

   i. The Offeror shall provide only new equipment unless otherwise expressly approved, in writing, by the DHS Contracting Officer. Offerors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

   ii. The Offeror shall be excused from using new OEM (i.e., "gray market”, "previously used") components only with formal Government approval, in writing, from the DHS Contracting Officer. Such components shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

iii. All equipment obtained by the Offeror on behalf of the Government will need to be provided to OCIO for review to validate requirements and approved Contractors by DHS.

c. Hardware and Software Requests

i. The contractors supply the Government hardware and software will provide the manufacturer's name, address, state, and/or domain of registration, and the DUNS number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNS number of those suppliers must be provided.

ii. Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors will perform due diligence to ensure that these standards are met.

iii. The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

1. For software products, the Offeror shall provide all OEM software updates to correct defects for the life of the product (i.e., until the "End of Life (EoL)"). Software updates and patches shall be either: made available to the government for all products procured under this Contract, replaced upon End of Support (EoS) is reached, or formally waived (in writing) by the DHS Contracting Officer.

d. Supply-Chain Transport

i. Offerors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill Contract obligations with the Government.

ii. All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the Contract, the period of performance, or one calendar year from the date the activity occurred.

iii. This transit process shall minimize the number of times in route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

iv. All records pertaining to the transit, storage, and delivery shall be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

v. The Offeror is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government.

vi. The Offeror shall provide a packing slip which shall accompany each container or package with the information identifying this solicitation number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

vii. The Offeror shall send a shipping notification to the intended government recipient; with a copy transmitted via email to the Contracting Officer, or designated representative. This shipping notification shall be sent electronically and will state this solicitation number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Notifications

i. The Offeror shall notify DHS Contracting Officer, COR and the Office of the Chief Information Officer and the DHS component Chief Information Officer through the Enterprise Security Operations Center (ESOC) directly of any suspected or potential violations of Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT) at NDAA_Incidents@hq.dhs.gov.

f. Foreign Equities

The Offeror shall immediately notify the DHS Contracting Officer, COR that will report to the Office of the Chief Security Officer (OCSO) or cognizant component personnel security office regarding any changes to corporate foreign ownership, control, or influence.

9.6 HSAR 3052.204-71 CONTRACTOR EMPLOYEE ACCESS. (SEPT 2012)

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

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

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(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 sensitive information or IT 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 sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

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

(End of clause)

10. PROPERTY

Accountable Personal Property - An asset that meets one or more of the following criteria: (1) expected useful life is two years or longer and an asset value and/or acquisition cost of $5,000 or more; (2) that is classified as sensitive; (3) for which accountability or property control records are maintained; (4) Capitalized personal property, (5) Leased property that meets accountability standards, or (6) otherwise warrants tracking in the property system of record. Current accountable personal property information may be obtained through the OBIM Accountable Property Officer (APO) Office at OBIMProperty@obim.dhs.gov.

Capitalized personal property - non-expendable personal property with an acquisition cost over an established threshold and a normal life expectancy of two years or more. Current Capitalization Threshold information may be obtained through the OBIM APO Office at OBIMProperty@obim.dhs.gov.

Contract property - All property, both real and personal, that is used in the performance of a contract, and includes facilities, material, special tooling, special test equipment, and agency-peculiar property. Contract property refers to both Contractor-Acquired Property (CAP) and Government Furnished Property (GFP), in the possession of contractors.

CAP - Property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title.

Excess Personal Property - Personal property under the control of any Federal agency that is not required or needed for that agency’s needs, as determined by the head of the agency or designee.

GFP - Property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. NOTE: GFP may also be referred to as Government Furnished Equipment (GFE), the two terms are interchangeable.

Leased property - Property that is not owned by DHS, but that is leased by the Government under terms as stipulated in the lease agreement (this excludes the leasing of property by contractors in the performance of a contract).

Sensitive personal property - All items, regardless of value, that require special control and accountability due to unusual rates of loss, theft, or misuse, national security or export control considerations. Such property includes but is not limited to, weapons, ammunition, explosives, information technology equipment with memory capability, cameras, and communications equipment. Current sensitive personal property information may be obtained through the OBIM APO Office at OBIMProperty@obim.dhs.gov.

PHYSICAL INVENTORY
In addition to requirements provided under FAR § 52.245-1:

The Contractor, jointly with the OBIM APO Office on an annual basis, shall perform, record, and disclose physical inventory results of CAP and GFP.

The Contractor shall, on a monthly basis, perform, record, and disclose physical inventory results of CAP and GFP to the OBIM APO Office at OBIMProperty@obim.dhs.gov and COR.

As requested, inventory results will be completed, certified and submitted, in the timeframe defined at the time of request, to the OBIM APO Office at OBIMProperty@obim.dhs.gov and COR.

PROPERTY DISPOSAL
All documentation and goods are the property of the United States Government and, if applicable, the contractor shall return or destroy appropriately upon request. The contractor shall comply with applicable Government rules and regulations for disposal of Government property. Further, the contractor shall provide necessary information to the COR and the OBIM IT Property team at OBIMProperty@obim.dhs.gov for all excess property prior to taking any action.

LOST, STOLEN, DAMAGED OR DESTROYED (LDD) PROPERTY
Unless otherwise provided in the contract, the contractor is liable for LDD of contract property, except for reasonable wear and tear.

Any occurrence of LDD must be investigated and fully documented by the COR, who will promptly notify the CO. The contractor will submit a report of any incident of LDD contract property to the COR in accordance with FAR § 45.504, "Contractor's Liability," and as detailed below, as soon as it becomes known

When GFP or CAP property is LDD, the Contractor must report within 24 hours of discovery of the event to the COR who will initiate a Report of Survey. This document will be obtained from OBIM IT Property team at OBIMProperty@obim.dhs.gov.

A Report of Survey will be prepared, regardless of whether or not preliminary research of a LDD event indicates positive evidence of negligence, misconduct, or unauthorized use and the responsible individual refuses to admit pecuniary liability.

The Contractor must forward this document with all supporting documentation to the COR within 5 business days of the LDD event for review.
The COR must submit the completed package to OBIMProperty@obim.dhs.gov within 5 business days of receipt from the Contractor.
The Contractor and COR must supply all requested information and any subsequent requests for information.

11. CONTRACTOR PERSONNEL & CONTRACTOR SECURITY

N/A – Not applicable – no on-site requirement for contractor personnel.