U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)
STATEMENT OF WORK (SOW)
FOR
Office of the Chief Procurement Officer (OCPO)
Acquisition Workforce and Systems Support (AWSS)
Acquisition Systems Branch (ASB)
Application and Data Management Support Services
ERA Windows Server 2016 to 2022 Upgrade and ERA Application and Reporting Enhancements for CISA migration from Chief of Contracting Office (COCO) to Head of Contracting Activity (HCA)

September 30, 2024

Contents

1.0 BACKGROUND

The Department of Homeland Security (DHS) Office of the Chief Procurement Officer (OCPO) is seeking professional services to assist the Acquisition Systems Branch (ASB) in a server upgrade from Windows 2016 to 2022.

ASB plays a crucial role in delivering application development services to both mission-critical and business-related users across multiple networks within DHS to include emerging software and applications. ASB presently relies on Federal Risk and Authorization Management Program (FedRAMP) accredited cloud services, including Microsoft Office 365, and DHS Enterprise Cloud (DEC) - Azure.

The Enterprise Reporting Application (ERA) uses a SharePoint 2016 on-premises user interface. Resides in the DEC-Azure environment as a major application with Authority to Operate (ATO). OCPO manages all software applications to include security updates and patching within the ERA infrastructure. The DHS Office of the Chief Information Officer (OCIO) DEC-Azure manages Operating System (OS) level security updates and patches.

ERA serves not only as a platform for capturing and reporting metrics but also functions as a data warehouse/data cube with business intelligence, aiding OCPO in performance management, audit management, and organizational assessment of DHS and Component contracting activities.

Within ERA, SharePoint utilizes SQL Server Reporting Services (SSRS) as software add-ons. Additionally, ERA generates visualizations through Power BI. While ERA reports are SQL-based, C# is used to bring data in from SurveyMonkey and some other automations. For the applications, within ERA, JavaScript Object Notation (JSON) is utilized to transfer data from the database to the application. It is then parsed and displayed in Hypertext Markup Language (HTML).

ERA engages in both pushing and pulling data through ETL batch processing. It acquires contract line-item data from diverse DHS-internal procurement-related business systems, as well as federal systems including FPDS, CPARS, SAM, SurveyMonkey and GSA's Forecast of Contracting Opportunities Tool. It is important to note that CPARS data is restricted to information related to the evaluation process exclusively and excludes actual performance assessment data. ERA also accommodates SSRS reports requested by customers and functions as a resource for customers to generate their own reports using Power BI.

ERA application hosting and maintenance is performed by ASB and the DEC-Azure OCIO team. Information Systems Security Officer (ISSO) support services for ERA are provided under a separate contract and are outside the scope of this effort.

ATO package must be submitted every (3) years. Current ERA ATO expires September 28, 2026.

The Federal Information Processing Standards (FIPS) 199 determination classifies ERA as moderate for confidentiality, moderate for integrity, and moderate for availability.

2.0 SCOPE

This project encompasses new Windows Server 2022 environments and the subsequent migration of existing applications and data from current Windows Server 2016 environments. The migration will be executed with minimal disruption to operations, ensuring data integrity and application functionality. Provisioning of the servers will be conducted by Office of the Chief Information Officer (OCIO)

Servers Included:

- SharePoint Servers (4)
- SFTP Server (1)
- Power BI/SSRS Server (1)
- SQL Database Servers (2)
- SQL Database and Analysis Server (1)
- SQL Server for Integration Services (1)

The project will also entail modifying ERA applications and reports to support CISA migration as a COCO to an HCA.

Specifically, the Contractor is responsible for the following activities as identified in the tasks below:

3.0 OBJECTIVE

This objective is organized around the following key areas:

- Setup and migrate 10 ERA servers from Windows 2016 to Windows 2022
    - Six: Production
    - Two: Staging
    - Two: Development
- Modify 31 ERA applications and reports for the CISA migration from a COCO to and HCA.
- The server and reporting upgrades must be completed NTL June 30, 2025.

4.0 APPLICABLE DOCUMENTS

The following documents provide specifications, standards, or guidelines that must be complied with to meet the requirements of this contract:

- DHS Enterprise Architecture
- DHS Acquisition Management Directive 102-01, which includes the DHS Acquisition Instruction/Guidebook 102-01-001 and Appendix B Systems Engineering Lifecycle (SELC)
- DHS Management Directive 140-01, Information Technology Security Services
- DHS Management Directive 4300 Information Technology Systems Security
- DHS Management Directive 103-01 Enterprise Data Management Policy
- IEEE STD 829-1998: IEEE Standard for Software Test Documentation
- IEEE STD 830-1998: IEEE Recommended Practice for Software Requirements Specifications
- IEEE STD 1233-1998: IEEE Guide for Developing System Requirements Specifications
- NIST Special Publication 800-18 Revision 1: Guide for Developing Security Plans for Federal Information Systems
- NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments
- NIST Special Publication 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach
- NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Federal Information Systems and Organizations.
- NIST Special Publication 800-116 Revision 1: Guidelines for the Use of PIV Credentials in Facility Access
- NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, dated December 2011
- OMB Memorandum 11-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors
- 36 CFR Chapter XII Subchapter B Records Management
- DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems (Version 13.3, February 13, 2023)
- DHS Acquisition Management Directive 201-01, including Appendix B – DHS Systems Engineering Life Cycle (SELC)
- DHS Management Directive 4010.2 – Section 508 Program Management Office & Electronic and Information Technology Accessibility
- SNAP System Operating Procedures (SOP)

5.0 SPECIFIC REQUIREMENTS

The Contractor is obligated to offer IT project development, delivery, and operations and maintenance (O&M) support capabilities that align with current and emerging industry technology, standards, and best practices throughout the performance period. The services provided must offer optimal value to the Government, granting DHS the adaptability to address both present and future requirements. The project delivery capabilities must satisfy all the

specifications outlined in this section. The Contractor's proposal should outline their approach to complying with these requirements.

The Contractor must be capable of adjusting resources and services as needed in response to project management-related conditions that may necessitate schedule or priority changes. The Agile/Scrum methodology will be employed, and as a result, occasional adjustments will be necessary based on the targeted sprint velocity, which will be determined collaboratively by the contractor and Government leadership, in accordance with industry project management best practices.

Working closely with Government leadership, the contractor will execute the following tasks.

5.1 TASK 1: WINDOWS SERVER MIGRATION FROM 2016 to 2022

5.1.1 Pre-Migration Assessment and Planning

- Analyze current environment (hardware, software, configurations, dependencies, performance) for databases, SharePoint, and SQL Server.
- Check compatibility of existing components with Windows 2022 and target versions of SharePoint and SQL Server.
- Develop detailed migration plans for each component (sequencing, resource allocation, testing, rollback, risk mitigation).
- Inventory and document all existing SharePoint applications, customizations, workflows, and integrations.
- Inventory and document all existing SQL Server databases and ETL processes.

5.1.2 Environment Preparation

- Backup and Recovery: Implement a comprehensive backup strategy.
- Data Validation: Ensure data integrity and schema compatibility.
- Performance Optimization: Review and optimize database performance.
- New Environment Setup:
    - Set up Windows 2022 environments with required versions of SharePoint and SQL Server.
    - Configure services, permissions, and security.

5.1.3 Migration

- Database Migration:
    1. Migrate SQL Server databases using appropriate methods.
    2. Validate data integrity post-migration.
    3. Update and reconfigure ETL processes.
    4. Test and validate ETL processes.

- SharePoint Migration:
    1. Perform test migrations to validate the migration process and identify potential issues.
    2. Migrate SharePoint content, site collections, web applications, and customizations.
    3. Update workflows, integrations, and custom solutions.

- Upgrade Execution
    1. Set up a test environment to simulate migration and identify issues.
    2. Develop and test upgrade scripts and procedures.
    3. Execute data migration, ensuring integrity.
    4. Validate application integration in the new environment.

5.1.4 Post Upgrade Activities

- Monitoring & Optimization:
    1. Monitor performance of databases, ETL processes, and SharePoint.
    2. Analyze and optimize performance as needed (fine-tune queries, indexes, configurations).
- Support & Documentation:
    1. Provide ongoing support for users and address any issues.
    2. Conduct thorough testing of all migrated SharePoint components.
    3. Update documentation (configurations, schemas, procedures).

5.2 TASK 2: ERA APPLICATIONS AND REPORTING MODIFICATIONS FOR CISA MIGRATION

5.2.1 Applications and Reporting List

ERA Element
Acq 360
AFPIRS
BART
Close Out Rpts
CSOP
Comp Dash
CN
Contract Perf
CPO Dash

Data Qalt
ECFS Rpts
HCA Goal
HCAST/R
Human Cap
One-Bid
OSR Consolidated Forms
OSR Protests
OSR Claims/IAA/UC
OSR Reports
PALT
Pub Query
Rpts & Dash
Service
Small Bus Dash
Staffing Model
SSO
Exports
Imports
DHS.gov
DHS Connect
Daily Report (.gov)

5.2.2 Reporting Data Source, Design and Functionality Updates

- Create New Data Sources: Establish new data sources specifically for the stand-alone component, ensuring they point to the correct database or data repository.

- Update Report Data Sources: Modify the identified reports to utilize the new data sources, ensuring data integrity and accuracy.
- Update Report Layouts: Adjust report layouts and designs to reflect the stand-alone component's specific data and branding.

5.2.3 SharePoint Application Updates

- Modify Application Logic: Update the application code or configuration to accommodate the changes in data sources and report locations.

- Update Web Parts: If reports are displayed within SharePoint using web

parts, ensure the web parts are correctly configured to display the updated reports.

5.2.4 Deployment and Validation

- Deploy from the Development Environment to the Staging Environment: Deploy the updated reports, data sources, and SharePoint applications to a staging environment for thorough testing and validation.

- User Acceptance Testing (UAT): Engage users to perform UAT in the test environment to confirm the changes meet their needs and identify any issues.
- Production Deployment: Plan and execute the deployment of the updates to the production environment, following established change management procedures.

5.2.5 Documentation

- Update Report Documentation: Revise any existing report documentation to reflect the changes in data sources, report design, and functionality.

- SharePoint Application Documentation: Update documentation for the affected SharePoint applications, outlining the modifications made and any impact on users.

6.0 TIMELINE

The server upgrade and ERA application and reporting enhancementsmust be completed NTL June 30, 2025.

7.0 DHS ENTERPRISE ARCHITECTURE COMPLIANCE

All services shall meet DHS Enterprise Architecture (EA) policies, standards, and procedures. Specifically, the Contractor shall monitor and assist in compliance to the extent applicable with the following Homeland Security (HLS) EA requirements:

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

- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Architecture Division (EAD) for review, approval and insertion into the DHS Data Reference Model and Mobius.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

7.1 INSTRUCTIONS FOR CONTRACTOR DISCLOSURE OF VIOLATIONS (SEP 2012)

When making a written disclosure under the clause at FAR 52.203-13, paragraph (b)(3), the Contractor may submit the disclosure to the Department of Homeland Security Office of Inspector General using the methods described at https://www.oig.dhs.gov/hotline or https://www.oig.dhs.gov/reports/publications/annual/contractor-disclosure, and submit the disclosure electronically to the Department of Homeland Security Office of Inspector General. The Contractor shall provide a copy of the disclosure to the Contracting Officer by email or facsimile on the same business day as the submission to the Office of Inspector General. The Contractor shall provide the Contracting Officer a concurrent copy of any supporting materials submitted to the Office of Inspector General.

7.2 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.

7.3 INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

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

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules 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.

7.3 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);

(vi)Contract clearance level;

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

(viii)Government programs, platforms, or systems involved;

(ix)Location(s) of incident;

(x)Date and time the incident was discovered;

(xi)Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;

(xii)Description of the government PII or SPII contained within the system; and

(xiii)Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

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

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

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

(i)Inspections;

(ii)Investigations;

(iii)Forensic reviews;

(iv)Data analyses and processing; and

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

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

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

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

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

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

7.4 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.

Contractor Employee Access (HSAR 3052.204-71)

(a) *Sensitive Information,* as used in this clause, means 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, Pub. L. 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.

(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.

7.5 Privacy Training (FAR 52.224-3)

(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 24.3 and 39.105).

(c) (1) "Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover-

(i) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;

(ii) The appropriate handling and safeguarding of personally identifiable information;

(iii) The authorized and official use of a system of records or any other personally identifiable information;

(iv) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access personally identifiable information;

(v) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and

(vi) The procedures to be followed in the event of a suspected or confirmed breach of a system of records or the unauthorized disclosure, access, handling, or use of personally identifiable information (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).

(2) Completion of an agency-developed or agency-conducted training course shall be deemed to satisfy these elements.

(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.

8.0 CONTRACTOR SECURITY LANGUAGE

SECURITY

Contractor access to unclassified and sensitive but unclassified information may be required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

Requests for Exception to U.S. Citizenship Requirement

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or through the DHS Office of the Chief Security Officer (OCSO). Components who have access may file their request via the Foreign National Vetting Management System (FNVMS), a part of the DHS OCSO Integrated Security Management System's (ISMS). For further information regarding the citizenship exception process, contact the DHS OCSO

This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

Post-Award Instructions Regarding Security Requirements for Non-Classified Contracts/Orders

The procedures outlined below shall be followed for the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD) to process background investigations, Entry on Duty determinations, and fitness determinations, as required, in a timely and efficient manner. Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS OCSO-HQS PSD. Prospective contractor employees shall complete and submit a combination of the below forms to the DHS OCSO-HQS PSD. The Standard Form (SF) 85 must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85 signature pages and other completed forms must be given to the OCSO-HQS PSD no less than

thirty days before the start date of the contract or thirty (30) days prior to the requested entry on duty date, for all contractor employees whether a replacement, addition, subcontractor employee, or vendor. OCSO-HQS PSD does not process any requests until the contract has been awarded and released from PRISM to FPDS and ERA by extension.

a. Standard Form (SF) 85 Questionnaire for Public Trust Positions
    i. SF-85P Certification
    ii. SF-85P Authorization for Release of Medical Information
b. FD Form 258 Fingerprint Card (2 copies) or Identity Enrollment Services
c. DHS Form 11000-6 Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement
d. DHS Form 11000-9 Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act
e. OF-306 Form, Declaration for Federal Employment

Only complete packages will be accepted by the DHS OCSO-HQS PSD. Specific instructions on submission of packages will be provided upon award of the contract.

The DHS OCSO-HQS PSD may, as it deems appropriate, authorize, and grant a favorable Entry on Duty (EOD) decision based on preliminary checks. A favorable EOD decision allows a contractor employee to commence work temporarily prior to the completion of the full background investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable fitness determination will follow. In addition, a favorable EOD or fitness determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD or fitness determination by the DHS OCSO-HQS PSD.

Limited access to Government buildings is allowable without an EOD decision if the Contractor is escorted by a Government employee and the purpose of the visit is to attend a limited number (less than 5) of required briefings or nonrecurring meetings in order to facilitate the transition of a contract. The intent of this statement is to allow a minimum amount of meetings/transition attendances to prepare for a new contract.

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

When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated

background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Depa1iment security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

- Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.
- Your POC at the Security Office is:

  DHS OCSO/PSD Security Customer Service Center
  Telephone: (202) 447-5010
  E-mailbox: [redacted]

9.0 SECTION 508 REQUIREMENTS

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

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

9.2 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.

10.0 PERIOD OF PERFORMANCE

The period of performance for this order is a nine (9) month period:

Period of Performance: September 30, 2024 through June 30, 2025

11.0 PLACE OF PERFORMANCE

The primary place of performance will be the Department of Homeland Security at 6595 Springfield Center Dr, Springfield, VA 22150.

In accordance with 41 U.S.C. 3306(f), DHS does not discourage a contractor from allowing its employees to telecommute/telework in the performance of Government contracts.

The Contractor may be permitted to work at an alternative work location/telework if the work being performed and required level of performance can be completed successfully in accordance with the contract requirements. The COR shall review and approve alternate work locations requests.

12.0 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 6:30 a.m. and 6:00 p.m. EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW. Any work outside of normal business hours and on weekends and Federal holidays must be approved by the COR prior to work being performed.

Federal Holidays include the following:

- New Year's Day - 1 January
- Martin Luther King's Birthday - Third Monday in January
- President's Day - Third Monday in February
- Memorial Day - Last Monday in May
- Juneteenth National Independence Day – 19 June
- Independence Day - 4 July
- Labor Day - First Monday in September
- Columbus Day - Second Monday in October
- Veterans Day - 11 November
- Thanksgiving Day - 4th Thursday in November
- Christmas Day - 25 December
- Any day specifically declared by the President of the United States of America as a national holiday.

If a holiday falls on Sunday, the following Monday will be observed as the legal holiday. When a holiday falls on a Saturday, the preceding Friday is observed as a legal holiday

by U.S. Government agencies.

13.0 TRAVEL

Contractor travel shall not be required.

14.0 WINDOWS SERVER MIGRATION DELIVERABLES

The contractor shall be responsible for the below deliverables for all services and support identified.

14.1 Pre-Migration Assessment and Planning (est. September 30 – November 30, 2024)

- Compatibility Assessment Report: A report detailing the compatibility of existing components with Windows 2022 and the target versions of SharePoint and SQL Server, including any identified issues or required upgrades.
- Migration Plan: A comprehensive plan for each component's migration, including sequencing, resource allocation, testing, rollback procedures, and risk mitigation strategies.

14.2 Environment Preparation (est. December 1-31, 2024)

- Backup and Recovery Plan: Documented backup strategy and procedures.
- Data Validation Report: A report documenting data validation results, ensuring data integrity and schema compatibility.
- Performance Optimization Report: A report detailing database performance review and optimization efforts.
- New Environment Setup Documentation: Documentation of the Windows 2022 environments with required versions of SharePoint and SQL Server, including configurations, services, permissions, and security settings.

14.3 Migration (est. January 1 – May 31, 2025)

- Database Migration Report: A report documenting the SQL Server database migration process, including validation results, ETL updates, and testing outcomes.
- SharePoint Migration Report: A report detailing the SharePoint migration process, including test migration results, content migration, workflow updates, and customization adaptations.
- Upgrade Execution Report: A report documenting the upgrade process, including test environment setup, script development and testing, data migration, and application integration validation.

14.4 Post Upgrade Activities (est. June 1-30, 2025)

- Monitoring & Optimization Reports: Regular reports on the performance of databases, ETL processes, and SharePoint, including any optimization actions taken.
- Support & Documentation Updates: Records of ongoing user support and issue resolution, as well as updated documentation on configurations, schemas, and procedures.

15.0 CISA MIGRATION APPLICATION AND REPORTING DELIVERABLES

15.1 Reporting Updates

- Updated SSRS reports with new data sources and modified layouts
- Newly created SSRS reports for the stand-alone component (if required)

15.2 SharePoint Application Updates

- Updated SharePoint applications with modified code or configuration
- Updated web parts (if applicable)

15.3 Testing and Validation

- Test plan and test results for all updated components

15.4 Documentation

- Updated report documentation
- Updated SharePoint application documentation

16.0 Other Terms and Conditions

All terms, conditions, and clauses from the overarching BPA automatically flow down to this BPA Call.

16.1 BPA Call Type

This is a Firm-Fixed-Price (FFP) BPA call.

16.2 Invoicing

CLIN 0001 ONLY

Invoices shall be prepared in accordance with Federal Acquisition Regulation (FAR) 52.212-4,

Contract Terms and Conditions – Commercial Items. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:
a) Cover sheet identifying DHS;
b) BPA Call and associated BPA Number;
c) Modification Number, if any;
d) DUNS Number;
e) Dates of provided services;
f) Associated Contract Line Item Number (CLIN); and
g) Associated Labor Category and hours performed.

Invoices shall be submitted electronically to [redacted] with a courtesy copy to the Contracting Officer [redacted], and the COR.

CLIN 0002 ONLY
In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1. Cover sheet identifying DHS;
2. Task Order Number;
3. Modification Number, if any;
4. UEI Number;
5. Month services provided
6. CLIN and Accounting Classifications
7. Contract Line Item Number (CLIN) and description for each billed item.
8. Any additional backup information as required by this contract.
9. ATTN: CISA/MBSO

The contractor shall submit invoices monthly for CISA's portion of expenses. The Contractor shall submit the invoice electronically to the address below:

E-mail: [redacted]

Simultaneously the Contractor shall provide an electronic copy of the invoice to the following individuals at the addresses below:

E-mail:
[redacted]

16.3 Points of Contact

16.3.1 Contracting Officer
The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds and authorize revisions of the terms and conditions of this BPA call. The Contracting Officer shall authorize any such revision in writing. If the Contractor makes any BPA call changes at the direction of any person other

than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the BPA call to cover any increases in changes that may result.

The Contracting Officer has the authority to perform any and all post-award functions in administering and enforcing the BPA call in accordance with its terms and conditions.

The Contracting Officer is:
[redacted]
DHS Office of Procurement Operations
E-mail: [redacted]

16.3.2 Contracting Officer's Representative (COR)
The Contracting Officer will designate a COR to assist in monitoring the work under this BPA call. The COR is responsible for the technical administration of the BPA call and technical liaison between the Contractor and the Government. The COR is not authorized to change the scope of work or specifications stated in the BPA call, to make any commitments, or otherwise obligate the Government or authorize any changes which affect the BPA call price, delivery schedule, period of performance, or other terms and conditions.

The Contracting Officer's Representative is:
[redacted]
DHS Office of the Chief Procurement Officer
Phone: [redacted]
E-mail: [redacted]