Department of Homeland Security (DHS)

Measurement and Evaluation (MEL)

Support Services

Statement of Work (SOW)

For

The Office of the Chief Information Officer (OCIO)

Office of the Chief of Staff (CoS)

Diversity, Equity, and Inclusion (DEI)

Cybersecurity Internship Program (CSIP)

July 18, 2024

FOR OFFICIAL USE ONLY (FOUO)

1. GENERAL

1.1. BACKGROUND

Diversity, Equity, and Inclusion (DEI) Team is seeking measurement and evaluation (MEL) support for the Cybersecurity Internship Program (CSIP).

CSIP is a multi-phase internship and retraining program managed by Office of the Chief Information Officer (OCIO)'s Diversity, Equity, and Inclusion program. The DEI program supports all technology organizations within the Department of Homeland Security (DHS). That is also its challenge to provide effective programming that fosters inclusion and creates opportunities for the organizations to work collaboratively to meet mission needs.

In order to ensure that CSIP is successful, it is imperative to measure and evaluate and iteratively improve based on the results of the evaluation.

1.2. SCOPE

The Contractor shall assist in providing all required resources and technical support services in accordance with the Government's requirements, per the methodology and technology specified by the Government, within the scope of this Statement of Work (SOW). The Contractor shall assist in providing Measurement and Evaluation (MEL) capabilities and provide demonstrated expertise in the following areas:

- Provide cradle to grave MEL services for the DEI team;
- Plan, develop, and manage measurement and evaluation work;
- Provide evaluation design to include data collection recommendations;
- Provide recommendations for objectives and key performance indicators (KPIs);
- Perform a variety of analyses required for the formulation, administration, and evaluation of a monitoring and evaluation system; (A project monitoring and evaluation (M&E) system covers all the work carried out during or after a project to define, select, collect, analyze, and use information)
- Provide measurement and evaluation of Government-Off-The-Shelf (GOTS) / Commercial-Off-The- Shelf (COTS) application recommendations to program;
- Provide program analysis, Project Management MEL support and program evaluation to include investigating the quality of program;
- Identify and recommend solutions to streamline processes and add efficiencies;
- Provide MEL Strategy, Policy, and Governance Support;
- Provide Strategic Communications Support for all measurement and evaluation work;
- Provide monthly updates and bi-annual evaluations of CSIP and its projects;
- Provide written reports as determined by schedule;
- The Contractor shall comply with all DHS standards and regulations including, but not limited to those for development, performance, testing, project management, operations support, security, architecture, and 508 Accessibility.

1.3. OBJECTIVE

The objective of this requirement is to provide MEL services to the DEI Team.
The scope of the services required under North American Industry Classification System

(NAICS) 541512 include:

- Measurement and evaluation services
- Communication and outreach
- Assisting with training support
- User guides, governance, and system documentation

The program's goal is to use MEL development approaches, methodologies, and best practices to review and improve capabilities and services.

2. APPLICABLE DOCUMENTS

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

- DHS Acquisition Management Directive 102-01, including Appendix B -DHS Systems Engineering Life Cycle (SELC)
- DHS Management Directive 4010.2- Section 508 Program Management Office &Electronic and Information Technology Accessibility
- National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53

3. SPECIFIC REQUIREMENTS/TASKS

The Contractor shall provide technical experts and services to perform, accomplish, and complete the tasks described herein. The following task statements are meant to be descriptive, not specific. The specific work shall be in accordance with and within the scope of the subsequent paragraphs. The Contractor shall provide technical support services based on current and evolving industry standards and best practices over the period of performance. The services delivered shall provide the best value to Government, allowing DHS the flexibility to meet current and future requirements. In close coordination with Federal leadership, the contractor shall perform the following tasks:

3.1 TASK ONE: Measurement and Evaluation Support (CLIN 0001)

The Contractor shall assist the DEI team by performing a range of measurement and evaluation activities, according to the Government's requirements and per the methodology specified. The Contractor shall demonstrate expertise in program strategy, organizational change, and business and data analysis. This support shall focus on team activities to include measurement, evaluation, metrics, analysis, and recommendations for improvement support. The Contractor shall assist in performing activities to include, but not limited to, the following:
Provide cradle to grave measurement and evaluation services for the
DEI team;
Plan, develop, and manage measurement and evaluation work;

Provide evaluation design to include data collection recommendations;
Provide recommendations for objectives and key performance indicators;
Perform a variety of analyses required for the formulation, administration, and evaluation of a monitoring and evaluation system; (A project monitoring and evaluation (M&E) system covers all the work carried out during or after a project to define, select, collect, analyze, and use information)
Provide measurement and evaluation Government-Off-The-Shelf (GOTS) / Commercial-Off-The-Shelf (COTS) application recommendations to program;
Provide program analysis, Project Management MEL support and program evaluation to include investigating the quality of program;
Identify and recommend solutions to streamline processes and add efficiencies;
Provide MEL Strategy, Policy, and Governance Support;
Provide Strategic Communications Support for all measurement and evaluation work;
Provide monthly updates and bi-annual evaluations of CSIP and its projects;
Provide written reports as determined by schedule;
Provide support in developing strategic MEL activities to support future planning, assist in developing strategic plans and roadmaps to meet emerging program and data integration needs to transform the current program state to an improved and effective target state;
Assist in the development of briefings, agendas, and other general documentation including training material and demonstration sessions for new and existing technologies to various DHS stakeholders;
Assist in the supporting a continuous improvement process by providing recommendations on improving products, services, and processes.

4. CONTRACTOR PERSONNEL

4.1. Qualified Personnel

The contractor shall be responsible for employing technically qualified personnel to perform the work specified in this statement of work. The contractor shall maintain the personnel, organization, and administrative control necessary to ensure that the work performed and delivered meets the government's established specifications and requirements. The work history of each contractor employee must contain adequate experience directly related to work he/she is required to perform under this task order. Adequate experience is defined as 3 or more years performing related work, he/she is required to perform under this task order.

The Government may conduct an administrative review, during the life of this order, to evaluate work histories on any contractor employee for the purposes of validating compliance with the above requirements; additionally, the government may conduct reviews and approval of resumes for proposed contractor personnel to be assigned to this task order. In addition, the Contractor must have demonstrated the ability to reach out to a wide variety of subject matter experts in relevant fields, retain their services, and productively engage them in support of government requirements.

The contractors shall provide resources that can meet the minimum DHS security standards and are available to work at a Government facility.

4.2. Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is always maintained. The Contractor shall ensure all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the (COR) prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

4.3. Key Personnel

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer.

Senior Analyst will be a Key person.

Contractor *Key* personnel may not be assigned by the Contractor to more than one key position for this requirement.

4.4. Senior Analyst

The Contractor shall provide a Senior Analyst who shall be responsible for all Contractor work performed under this SOW. The SENIOR ANALYST shall be a single point of contact for the Contracting Officer and the COR. It is anticipated that the SENIOR ANALYST shall be one of the senior level employees provided by the Contractor for this work effort. The name of the SENIOR ANALYST, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the SENIOR ANALYST, shall be provided to the Government as part of the Contractor's proposal. The SENIOR ANALYST is further designated as *Key* by the Government. During any absence of the SENIOR ANALYST, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. The SENIOR ANALYST and all designated alternates shall be able to read, write, speak and understand English. Additionally, the Contractor shall not replace the SENIOR ANALYST without prior approval from the Contracting Officer. One Senior Analyst will be designated as a Key Personnel.

The SENIOR ANALYST shall be available to the COR via telephone between the hours of 8am and 6pm ET, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 2 hours of notification.

4.5. Employee Identification

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is always not readily apparent and display all identification and visitor badges in plain view above the waist.

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and always display the Government issued badge in plain view above the waist.

4.6. Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies, and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees always present a professional appearance and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations, and policies concerning safety and security.

4.7. Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the COR), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

5. OTHER APPLICABLE CONDITIONS

5.1. SECURITY

Contractor access to unclassified, but Security Sensitive Information may be required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

5.2. Compliance with DHS Security Policy Terms and Conditions

All hardware, software, and services provided under this task order must be compliant with DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017 and DHS Policy Directive 4300A, "Information Technology System Security Program, Sensitive Systems," version 13.3, February 13, 2023.

5.3. Encryption Compliance Terms and Conditions:

If encryption is required, the following methods are acceptable for encrypting sensitive information:

- FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
- National Security Agency (NSA) Type 2 or Type 1 encryption.

5.4. Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security*. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information.
Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

5.5. Post-Award Instructions Regarding Security Requirements for Contracts/Orders

The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

Carefully read the security clauses in the Order. Compliance with the security clauses in the contract is not optional.

Contract 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 everyone 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 Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) days before the start date of the contract or thirty (30)
days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

Standard Form 85P, "Questionnaire for Public Trust
Positions" FD Form 258, "Fingerprint Card" (2 copies)

DHS Form 11000-6 "Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement"
DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Rep is Pursuant to the Fair Credit Reporting Act"

Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability 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 decision or suitability determination by the Security Office.

Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and non-recurring meetings in order to begin transition work.

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 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 Department security policy are subject to having their access to Department IT systems and facilities terminated, whether 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.

6. PERIOD OF PERFORMANCE

The period of performance for this contract is a twelve (12) month base period as follows:

Base Period: September 30, 2024 through September 29, 2025

7. PLACE OF PERFORMANCE

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.

At the discretion of the COR, the contractor may be authorized telework under this contract. If telework is authorized, the days and hours for telework shall be coordinated with the COR. The contractor shall follow OPM Guidance for Government closures, if telework is authorized. The contractor shall maintain their own telework policy for its employees. The primary place of performance will be the Department of Homeland Security located at 6th floor; TSA Headquarters 6595 Springfield Center Drive Springfield VA 22150.

8. CONTRACT TYPE

The anticipated contract type for this order is firm fixed price.

9. HOURS OF OPERATION

Except for Level 3 support, Contractor employees shall generally perform all work between the hours of 8:00 a.m. and 6:00 p.m. ET, 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. Level 3 support is any work outside of normal business hours and on weekends and Federal holidays. L3 support shall be approved by the COR prior to work being performed.
Recognized Holidays: The Contractor shall not perform work on the following recognized holidays unless specifically authorized by the COR on this contract. If work is authorized by the COR, the contractor shall not charge overtime for working on the Holiday.

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day/Indigenous
People's Day President's Day	Veterans' Day
Memorial Day	Thanksgiving Day
Juneteenth	Christmas Day
Independence Day	

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.

For other than firm fixed price contracts, the contractor will not be reimbursed when the government

facility is closed for the above reasons. The Contractor must always maintain an adequate workforce for the uninterrupted performance of all tasks defined within this contract when the Government facility is not closed for the above

reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

10. TRAVEL

Contractor travel shall not be required.

11. DELIVERABLES

11.1. Post Award Conference (Deliverable 1)

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR 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 and review the Contractor's draft project plan. The Post Award Conference will be held or via teleconference.

11.2. Project Plan (Deliverable 2 & 3)

The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 10 business days after the Post Award Conference.

11.3. Business Continuity Plan (Deliverable 4 &5)

The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 10 business days after the date of award and updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- How the Contractor will communicate with the Government during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
- Telephone numbers
- E-mail addresses

Individual BCPs shall be activated immediately after determining that an emergency has occurred. BCPs shall be operational within 4 hours of activation or as directed by the Government and shall be sustainable until the emergency is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life-threatening emergency, the COR shall immediately contact the Contractor Project Manager to ascertain the status of any Contractor personnel who were in Government controlled space affected by the emergency.

When any disruption of normal, daily operations occurs, the Contractor Project Manager and the COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- Essential Contractor work products expected to be continued, by priority

The Government and Contractor Project Manager shall make use of the resources and tools available to continue contracted functions to the maximum extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

11.4. Monthly Status Reports (MSR) (Deliverable 6)

The Contractor shall submit a monthly status report covering a 30-day period to the COR, Contracting Officer (CO) and Contract Specialist (CS). The monthly report shall contain a heading with the following information at a minimum: Contract number, Order number, Order Period of Performance, Contractor Name, Program Manager's name and telephone number, Order Award amount, Period of Performance being reported, and Date of submission. The Contractor shall deliver this report on the 10^{th} business day of every month. The Contractor shall assist DHS in compiling useful data on work performed under this Task Order. Each status report will contain the following support items:

- A brief, factual summary description of progress in accomplishing technical objectives stated in the SOW;
- For each task, provide: a summary of work completed, work in progress and work planned; and for labor hour tasks include hours/dollars expended for the reporting period and cumulatively and hours/dollars remaining;
- Updates to all Project Management Plans;
- Identify significant problems and their impacts, causes, proposed corrective actions; and the effect that such corrective actions will have on the accomplishments of the IDIQ order objectives;
- Status on degree of completion for tasks/activities described in all PMPs;
- Upcoming events; and
- ODC expenditure status.

11.5. MEL Reports (Deliverable 7)

The contractor shall create MEL reports for at least bi-annually to document progress of the MEL work being performed. These documents shall be created in accordance with DHS standards and using appropriate templates. If template does not exist, the contractor shall follow best industry

standards and create a template that can be used.

12. PROGRESS MEETINGS

The Project Manager shall be responsible for keeping the COR informed about Contractor progress throughout the performance period of this contract and ensure Contractor activities are aligned with DHS objectives. At a minimum, the Project Manager shall review the status and results of Contractor performance with the COR on a monthly basis by telephone or at government office.

13. GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows and Microsoft Office Applications).

14. 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.

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

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

1.1 Section 508 Requirements for Technology Services

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

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

3. When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The Contractor shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at https://www.dhs.gov/trusted-tester.

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

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

1.2 Section 508 Deliverables

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

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

3. **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.

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

- Documentation of features provided to help achieve accessibility and usability for people with disabilities.
- Documentation on how to configure and install the ICT Item to support accessibility.
- Documentation of core functions that cannot be accessed by persons with disabilities.
- Documentation of remediation plans to address non-conformance to the Section 508 standards

15. DHS ENTERPRISE ARCHITECTURE (EA) COMPLIANCE

All solutions and services shall meet DHS Enterprise Architecture policies, standards, andprocedures. Specifically, the contractor shall comply with the following Homeland Security (HLS) EA requirements:
All developed solutions and requirements shall be compliant with the HLS EA principles.
All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile; all products are subject to DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the HLS EA 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 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the **corresponding declarations of conformance defined in the USGv6 Test Program.**

16.0 UNCLASSIFIED REQUESTS

ISO Terms and Conditions for Sensitive but Unclassified Requests

DHS Security Policy Requirement

The following terms and conditions should be included in all acquisition documents.
All hardware, software, and services provided under this task order must be compliant with DHS Information Security System Program 4300A version 13.3 Feb, 13 2023 and attachments.

Encryption Compliance Requirement

The following terms and conditions should be included in all acquisition documents.
1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2 and / or FIPS 140-3.

2. National Security Agency (NSA) Type 2 or Type 1 encryption.

3. Public Key Infrastructure (PKI), key cards, biometrics, or in the case of multi-factor authentication, some combination therein (See Attachment U) Information Security Sensitive Systems Program Directive 4300A version 13.3, Feb 2023.

Security Review Requirement

The following requirements should be included in all acquisition documents.

Security Review

The government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The contractor shall afford DHS,

including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COR), and other government oversight organizations, access to the contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The contractor will contact the Office of DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary 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 DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

Interconnection Security Agreement (ISA)

The following requirements should be included in the acquisition document if the service being supplied requires a connection to a non-DHS, contractor system, or DHS system of different sensitivity.

Interconnection Security Agreement Requirements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. Connections with other federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements. The applicable network connectivity policy is located in the Access Control Section, for "Interconnection Security Agreements," of the DHS 4300A, attachment N.

Required Protections for DHS Systems Hosted in Non-DHS Data Centers

The following requirements should be included in acquisition documents for information systems which are hosted, operated, maintained, and used on behalf of DHS at non-DHS facilities. Contractors are fully responsible and accountable for ensuring compliance with all Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST), Special Publication SP-800-47, DHS Management Directive 140-01, "Information Technology Security Program," Revision 2, May 5, 2017, Federal Information Processing Standard (FIPS) and related DHS security control requirements (to include configuration guides, hardening guidance, DHS Security Policy, Procedures, and Architectural guidance). The contractor security procedures shall be the same or greater than those that are provided by DHS Enterprise Data Center(s). Please note that all of the subsections from **Security Authorization** to **Log Retention** are included in this requirement in compliance with 4300A Information Security Systems Program version 13.3, Feb 13, 2023, attachment N.

Security Authorization

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.

At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these requirements. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the government, the contractor shall fully cooperate and facilitate in a government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture in accordance with applicable laws and DHS policies to the satisfaction of the DHS COR. Areas of consideration could include:

1. Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers
2. Compliance to DHS Identity Credential Access Management (ICAM)
3. Security reporting to DHS central control points (i.e., the DHS National Operations and Security Center (NOSC) and integration into DHS Security Incident Response
4. Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
5. Performance of activities per continuous monitoring requirements

Continuous Monitoring
The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

1. Asset Management
2. Vulnerability Management
3. Configuration Management
4. Malware Management
5. Log Integration
6. Security Information Event Management (SIEM) Integration
7. Patch Management
8. Providing near-real-time security status information to the DHS SOC

Specific Protections
Specific protections that shall be provided by the contractor include, but are not limited to the following:

Security Operations
The contractor shall operate a National Operations and Security Center (NOSC) to provide the security services described below. The contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The NOSC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility NOSC shall adhere to the incident response plan.

Computer Incident Response Services
The contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

Firewall Management and Monitoring
The contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Intrusion Detection Systems and Monitoring
The contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the Network Intrusions Detection Systems (NIDS) solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Physical and Information Security and Monitoring
The contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

Vulnerability Assessments
The contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

Anti-malware (e.g., virus, spam)
The contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall

notify the appropriate DHS point of contact in accordance with the incident response plan.

Patch Management

The contractor shall perform provide patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications for Host-based Intrusion Detection system (HIDS), (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

Supply Chain Risk Management Requirement

Supply Chain risks result from adversarial exploitation of the organizations, people, activities, information, resources, or facilities that provide hardware, software, or services. These risks can result in a loss of confidentiality, integrity, or availability of information or information systems. A compromise to even minor system components can lead to adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.

Authorities:

Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply Chain Risk Management
Department of Homeland Security, Security Policy for Sensitive Systems 4300A
Homeland Security Presidential Directive 23, Cyber Security and Monitoring, 8 January 2008
Office of Budget and Management Circulation A-130, Appendix III
National Institute of Standards and Technology, Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

Supply Chain Risk Management

The following requirements should be included in all hardware and software requests to ensure the confidentiality, integrity, and availability of government information.
The contractors supplying the government hardware and software shall provide the manufacture's name, address, state and/or domain of registration, and the Data Universal Numbering System (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 also be provided.
Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.
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.
Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.
The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.
The Supply Chain Risk Management Plan must address the following elements:
1. How risks from the supply chain will be identified,
2. What processes and security measures will be adopted to manage these risks to the system or system components.
3. How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan must remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan will be provided to the Contracting Officer Technical Representative (COR) 30 days post award.
The contractor acknowledges the government's requirement to assess the contractors Supply Chain Risk posture. The contractor understands and agrees that the government retains the right to cancel or terminate the contract, if the government determines that continuing the contract presents an unacceptable risk to national security.
The contractor must disclose, and the government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.
The contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the government. If a shipped OEM part fails, all replacement parts must be OEM parts.

The contractor shall be excused from using new OEM (i.e., "grey market," previously used) components only with formal government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e., until the "end of life."). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors 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.

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.

These records must be readily available for inspection by any agent designated by the US Government as having the authority to examine them.

This transit process shall minimize the number of times in route components undergo a change of custody and make use 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.

The contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the government. The contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

Definitions

As used in this contract or clause–

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

End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).
End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).
Information and Communications Technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).
Product: part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.
Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product:
i. The contractor must provide new equipment unless otherwise formally approved by the government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the government. In the event that a shipped OEM product, or part or component of that product, fails, all replacements must be new (i.e., non-refurbished, not previously used) OEM.
ii. The contractor may provide previously used OEM products only with written government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.
Accounting of Components in ICT Products:
i. The contractor shall provide and maintain a list of components for each

product used in performance of the contract, including through subcontracts or other arrangements. This list for each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.
ii. The contractor shall notify the government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to

reflect the new version of the software. This includes software builds to integrate an updated component or dependency.
iii. For software products, the contractor must provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract and replaced when End of Support (EoS) is reached.
iv. A contractor using team members in performance of the contract (e.g., subcontractors or other service providers) shall ensure that the standards for the accounting of components in this subsection are met by team members.
Supply-Chain Transport:
i. The contractor shall use formal, documented and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.
ii. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance and make available for inspection upon request of the government.
iii. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.
iv. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.
v. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.
Changes to Ownership and Control: The contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any significant changes to corporate ownership or control from contract award through final delivery or the end of the period of performance. A significant change would be one in which a change occurs in the individuals or entities who, directly or indirectly, either (1) exercises substantial control over an entity, or (2) owns or controls at least 25 percent of the ownership interests of an entity.
If the ITAR request is for products, systems, services, hardware, or software that enables access to controlled facilities and information systems, please include the PIV Credential Compliance requirement below.

Examples of when to use this requirement:
• The ITAR request is for a Commercial-Off-The-Shelf (COTS) product that

the component requires to fulfill its mission requirements. The COTS product must be enabled to use PIV credential, in accordance with NIST guidelines including Federal Information Processing Standard Publication (FIPS) 201 (Demonstrated progress toward integration with AppAuth would be considered a confirmation to PIV enablement).
• The ITAR request is for the procurement of 1500 desktops as part of a

technology refresh. The desktops must have a PIV card reader.
• The component is requesting a custom software product to be developed.

The custom software product must be able to use PIV credential for authentication purpose.
Federal Risk and Authorization and Management Program
This language can be applied to the acquisition of information technology, which includes operational technology, by or for the use of DHS or components except for acquisitions of information technology for national security systems. Acquisitions of information and operational technology for national security systems shall be conducted in accordance with 40 U.S.C. § 11302 for performance requirements and results-based management; the role of the agency Chief Information Officer in acquisitions; and accountability. These requirements are addressed in OMB Circular No. A-130.39.002
• A clause substantially the same as this language should be inserted in

solicitations and contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services, except for acquisitions of information technology for national security systems. This includes all contracts and solicitations where:
• A contractor or subcontractor provides equipment, software or services that,

process, store, or transmit government data.

• A contractor or subcontractor provides information system(s) used or operated,

by a federal agency, or a contractor, or other organization on behalf of the agency; this includes information systems that control, operate, or interface with operational technology.
Subcontracts. The contractor shall include the substance of this clause in subcontracts under this contract at all tiers (including subcontracts for the acquisition of commercial items), in which the subcontractor provides devices, software or services that process, store or transmit government data; or provides information system(s) used or operated by a federal agency, or a contractor, or other organization on behalf of the agency; this includes information systems that control, operate, or interface with operational technology. All references to the contractor are applicable to all subcontractors. Subcontractors must also notify the prime contractor (or next higher-tier subcontractor) of all incident reporting.
Cloud computing. All use of cloud computing products or services that process unclassified information must comply with the FedRAMP Authorization Act, 44 U.S.C. Section 3607 et. seq. The following requirements apply when using cloud computing to provide information systems or services in the performance of the contract.
Cloud computing security requirements. The contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with FedRAMP Security Authorization Requirements unless notified by the Contracting Officer that this requirement has been waived by the Agency Chief Information Officer.
Cloud computing continuous monitoring. The contractor shall maintain an adequate continuous monitoring capability based on the FedRAMP Security Authorization Requirements including processes described in the NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations and governed by the FedRAMP Continuous Monitoring Strategy Guide.
Cloud computing services cyber incident reporting. The contractor shall report all cybersecurity incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted according to FedRAMP Security Authorization Requirements, published FedRAMP Incident Communications Procedures, and Federal Incident Notification Guidelines for submitting incident notifications to CISA using the CISA incident reporting form (https://us-cert.cisa.gov/report).
Malicious software. The contractor that discovers and isolates malicious software in connection with a reported cybersecurity incident shall submit a report regarding the malicious code, and any additional data as requested, to the Contracting Officer (and

any other entities in accordance with any established agency procedures). The contractor shall also submit a malware report to CISA via the incident reporting form (https://us-cert.cisa.gov/report) and malicious code samples or artifacts to CISA using the appropriate form at https://www.malware.us-cert.gov.

Access to additional information or equipment necessary for forensic analysis. Upon request by the Agency or CISA, the contractor shall provide the government with access to additional information or equipment that is necessary to conduct a forensic analysis. The contractor and subcontractors shall agree to provide full access and cooperation for all activities determined by the government to be required to (1) ensure an effective incident response or (2) investigation of potential incidents. To facilitate these activities, the contractor shall deploy login and consent banners on all systems and networks that are federal information systems or support the execution of the contract that are consistent with CISA's guidance on consent banners, found at https://www.cisa.gov/publication/guidance-consent-banners.

Limitations on access to, use and disclosure of federal data and federal metadata. The contractor shall not access, use, or disclose federal data unless specifically authorized by the terms of this contract or a task order or delivery order issued hereunder.

If authorized by the terms of this contract or a task order or delivery order issued hereunder, any access to, or use or disclosure of, federal data shall only be for purposes specified in this contract or task order or delivery order.

The contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of this contract.

The contractor shall use federal metadata only to manage the operational environment that supports the federal data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

Notification of third-party access requests. The contractor shall notify the Contracting Officer promptly of any requests from a third party for access to federal data or federal metadata or access to information systems with access to federal data or metadata, including any warrants, seizures, or subpoenas it receives, including those from another federal, state, or local agency, with the exception of requests made by CISA as part of paragraph (f) above. The contractor shall cooperate with the Contracting Officer to take all measures to protect federal data and federal metadata from any unauthorized disclosure.

Definitions
As used in this contract or clause–
Adequate Security: 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.
Source: OMB Circular A-130
Cloud computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This is typified by characteristics such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It includes service models such as software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.
Source: FedRAMP
Covered Telecommunications Equipment or Services: The term ''covered telecommunications equipment or services'' means any of the following:
• Telecommunications equipment produced by Huawei Technologies Company

or ZTE Corporation (or any subsidiary or affiliate of such entities).
• For the purpose of public safety, security of government facilities, physical

security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
• Telecommunications or video surveillance services provided by such entities or

using such equipment.
• Telecommunications or video surveillance equipment or services produced or

provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Source: Section 889, 2019 Defense Authorization Act

Cybersecurity Directives: compulsory directions from the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency to an agency in the form of either Binding Operational Directives or Emergency Directives, including any supplemental direction thereto. Binding Operational Directives are issued for the purposes of safeguarding federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; shall be in accordance with policies, principles, standards, and guidelines issued by the Director of the Office of Management and Budget; and may be revised or repealed by the Director if the direction issued on behalf of the Director is not in accordance with policies and principles developed by the Director. Emergency Directives are issued in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency. Emergency Directives direct an agency to take lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

Source(s): 44 U.S.C. §§ 3552, 3553(b)(2), 3553(h)

Federal contract information: Information, not intended for public release, that is provided by or generated for the government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as on public websites) or simple transactional information, such as necessary to process payments. Source: FAR 52.204-21

Federal Information System: 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. Source: 40 U.S.C. § 11331

FedRAMP Security Authorization Requirements: the requirements and guidelines for security authorizations of cloud computing products and services, established and regularly updated by the FedRAMP Board (née JAB) and published by the Program Management Office (PMO); which include standardized baselines of security controls, privacy controls, and controls selected for continuous monitoring from NIST Special Publication 800-53 (as amended) as well as applicable Federal Information Processing Standards (FIPS), requirements and policies issued by Office of Management and Budget (OMB), and directives issued by the Department of Homeland Security (DHS) through the Cybersecurity & Infrastructure Security Agency (CISA).

High Value Asset (HVA): A designation of federal information or a federal information system when it relates to one or more of the following categories:
• **Informational Value** – The information or information system that processes, stores, or transmits the information is of high value to the government or its adversaries.
• **Mission Essential** – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.
• Federal Civilian Enterprise Essential (FCEE) – The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.
Source: OMB M-19-03

Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
Source: NIST SP 800-145

Incident: an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Source: 44 U.S.C. § 3551

Information: any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual.
Source: NIST glossary

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

Source: 44 U.S.C. § 3502
Information System Service: A capability provided by an information system that facilitates information processing, storage, or transmission.
Source: NIST glossary
Information technology: In lieu of the definition in FAR 2.1, the term "information technology"
• With respect to an executive agency means any equipment or interconnected

system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use - of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product.
• Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but
• Does not include any equipment acquired by a federal contractor incidental to a

federal contract.
Source: 40 U.S.C. § 11101(6)
Information Technology Product: A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.
Source: NIST glossary
Malware: Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity or availability of the victim's data, applications, or operating system. Source: NIST SP 800-83

Metadata: information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).
Modular Contracting: the use of one or more contracts to acquire information technology systems in successive, interoperable increments.
National security system means any telecommunications or information system operated by the United States Government, the function, operation, or use of which-
• Involves intelligence activities.
• Involves cryptologic activities related to national security.
• Involves command and control of military forces.
• Involves equipment that is an integral part of a weapon or weapons.

system; or
• Is critical to the direct fulfillment of military or intelligence missions.

• This does not include a system that is to be used for routine.

administrative and business applications, such as payroll, finance, logistics, and personnel management applications.
Operational Technology (OT): Operational technology, which is a subset of information technology. As defined by the IoT Cybersecurity Improvement Act, P.L 116-207, operational technology is hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise. OT encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, transportation systems, physical access control systems, monitoring systems, and measurement systems.
Source: Adapted from NIST SP 800-37 Rev. 2

Personal Identification Verification (PIV) Credential Compliance

Authorities:

• HSPD-12 "Policies for a Common Identification Standard for Federal Employees and contractors"
• OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and contractors"
• OMB M-06-16 "Acquisition of Products and Services for Implementation of HSPD-12"
• NIST FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and contractors"
• NIST SP 800-63 "Electronic Authentication Guideline"
• OMB M-10-15 "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"

Personal Identification Verification (PIV) Credential Compliance Requirement

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.
Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.
PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.
If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

20. OCIO CISO CYBER-SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) SOW LANGUAGE

a. Definitions
i. Component: a unit defined by the supplier that connects to and functions as part of the product. For software products, a component is a unit of software defined by a supplier at the time the component is built, packaged, or delivered. For hardware, a component is one hardware unit designed to connect to and function as part of a larger product.
ii. End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).
iii. End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).
iv. Information and Communications Technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

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

b. Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product
i. The contractor shall provide new equipment unless otherwise formally approved by the Government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the Government. In the event that a shipped OEM product, or part or component of that product, fails, all replacements must be new (i.e., non-refurbished, not previously used) OEM.
ii. The contractor may provide previously-used OEM products only with written Government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

c. Accounting of Components in ICT Products
i. The contractor shall provide and maintain a list of components for each product used in performance of the contract, including through subcontracts or other arrangements. This list for each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.
ii. The contractor shall notify the Government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to reflect the new version of the software. This includes software builds to integrate an updated component or dependency.

iii. For software products, the contractor shall provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract, and replaced when End of Support (EoS) is reached.
iv. A contractor using team members in performance of the contract (e.g., subcontractors or other service providers) shall ensure that the standards for the accounting of components in this subsection are met by team members.

d. Supply-Chain Transport
i. The contractor shall use formal, documented and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.
ii. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance, and make available for inspection upon request of the Government.
iii. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.
iv. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.
v. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.
e. Changes to Ownership and Control
The Contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any significant changes to corporate ownership or control from contract award through final delivery or the end of the period of performance. A significant change would be one in which a change occurs in the individuals or entities who, directly or indirectly, either (1) exercises substantial control over an entity, or (2) owns or controls at least 25 percent of the ownership interests of an entity.

21. GOVERNMENT TERMS & DEFINITIONS

21.1 CO – Contracting Officer

21.2 COR – Contracting Officer's Representative

21.3 DHS - Department of Homeland Security

21.4 MD – Management Directive

21.5 PSB – Platform Solutions Branch

21.6 SDD – Solutions Development Directorate

21.7 SOW – Statement of Work

21.8 GFR – Government Furnished Resources

21.9 PCII – Protected Critical Infrastructure Information

21.10 COTS – Commercially-Off-The-Shelf

22. GOVERNMENT FURNISHED RESOURCES

The Government will provide the workspace, equipment, and supplies necessary to perform the on-site portion of Contractor services required in this contract, unless specifically stated otherwise in this work statement.

The Contractor shall use Government furnished facilities, property, equipment and supplies only for the performance of work under this contract and shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear.

The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

23. CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment, and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in Section 22.

24. GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

The COR will have **10 business days** to review deliverables and make comments. The Contractor shall have **5 business days** to make corrections and redeliver.

All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

25. DELIVERABLES

The Contractor shall consider items in **BOLD** as having mandatory due dates. Items in *italics* are deliverables or events that must be reviewed and/or approved by the COR prior to proceeding to next deliverable or event in this SOW.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	11.1	***Post Conference Award***	10 Business Days After Award	N/A
2	11.2	***Draft Contractor Project Plan***	At Post Award Conference	COR, Contracting Officer, and Contract Specialist
3	11.2	***Final Contractor Project Plan***	10 Business Days After Post Award Conference	COR, Contracting Officer, and Contract Specialist
4	11.3	***Original Business Continuity Plan***	10 Business Days After Award	COR, Contracting Officer, and Contract Specialist
5	11.3	***Updated Business Continuity Plan***	Not Applicable	COR, Contracting Officer, and Contracting Specialist
6	11.4	**Monthly Status Reports**	The 10th calendar day of each month for the preceding month's activities	COR, Contracting Officer, and Contracting Specialist
7	11.5	**MEL Reports**	10 Business Days after deployment; the 15th calendar day of the seventh month for the first six month's activities	COR, Contracting Officer, and Contracting Specialist

26. CONTRACT ADMINISTRATION INSTRUCTIONS

26.1 Government Administration Points of Contract

The Contracting Officer's Representative (COR) for the IDIQ order is a Government official who has been delegated specific responsibilities by the Contracting Officer. The COR will be assigned in writing by the Contracting Officer. For this effort the COR is:

[redacted]

a) The Government Contracting Officer (CO): [redacted]

b) The Government Contract Specialist (CS): Name: [redacted]

26.2 COR Responsibility

The CO within its authority may designate in writing one or more government employees, by name and position title, to take action for the contracting officer under this IDIQ order. Each designee shall be identified as a COR.

The COR will represent the CO in the administration of technical details within the scope of the IDIQ order. The COR is also responsible for the final inspection and acceptance of all IDIQ order deliverables and reports, and such other responsibilities as may be specified in the IDIQ order. The COR is not otherwise authorized to make any representations or commitments of any kind on behalf of the CO or the Government. The COR does not have authority to alter the contractor's obligations, or to change the IDIQ order specifications, price, terms, and conditions. If, as a result of technical discussions, it is desirable to modify IDIQ order obligations or the specification, changes will be issued in writing and signed by the CO. The COR will be assigned in writing by issuance of a formal appointment letter from the CO.

26.3 Invoice Procedures

The Contractor shall submit a proper invoice for the services performed and completed, no later than the 15th calendar day of the month following the reporting period in accordance with FAR 52.232-1 Payments. Invoice payment shall be made upon satisfactory contractor performance provided and required deliverables are accepted and approved by the Government.

Invoices shall be for services incurred against the work performed during the previous month's period of performance which shall begin on the first of the month and end on the last day of the month.
All invoices shall be submitted by the Contractor in electronic format via email. No other form of invoice submission will be accepted. Invoices shall be electronically submitted to the following addresses:

The subject line of the electronic mail message shall contain the following information: Contractor Name, Contract/Order Number, Contractor's Invoice Number; as well as Month and Year of Invoice Billing.

Failure to comply with the procedures outlined may result in payment being delayed at no additional cost to the Government.