PR# PCCA-24-00057
Solicitation # 70RCSJ24Q0000058

DEPARTMENT OF HOMELAND SECURITY (DHS)
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)
Office of Chief Acquisition Executive (OCAE)
STATEMENT OF WORK
Procurement Organization and Policy Support

1.0 GENERAL

1.1 BACKGROUND

The CISA Act of 2018 created the Cybersecurity and Infrastructure Security Agency (CISA) within DHS. CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. Our partners in this mission span the public and private sectors, with CISA serving as the foundation to mobilize the col508lective defense and leader of the Nation's efforts to understand and manage the risk to our critical infrastructure. CISA includes the Office of the Director (OD), Mission Enabling Offices (MEOs) and the following Divisions: The Cybersecurity Division (CSD), Infrastructure Security Division (ISD), Emergency Communications Division (ECD), Integrated Operations Division (IOD) and the National Risk Management Center (NRMC), which are headquartered in the National Capital Region (NCR).

The purpose of this SOW is to secure subject matter experts in providing strategic planning, and training for CISA on behalf of OCAE. OCAE is one of the CISA's MEO offices providing policy, guidance, oversight and support for Acquisition an5d Contracts Agency wide. CISA is striving to grow and expand a mature OCAE cadre of contract and acquisition professionals. Additionally, OCAE goals include mentoring, and training contracting officer representatives and project managers throughout the operational divisions.

1.2 SCOPE

The scope of this SOW supports the OCAE office in its respective responsibilities throughout CISA, which includes the Chief of Contracting Office (COCO). CISA COCO requires continued expert CISA acquisition organization development, acquisition training, and contract consolidation support as it continues to lead the CISA-wide acquisition transformation and maturation. The contractor will be responsible for assisting in strategic planning support; training in DHS and CISA policy; documenting acquisition and contract processes; creating and facilitating monthly acquisition and contract community of practice sessions; and providing reports and briefings on relevant subject matter such as policy briefs.

1.3 APPLICABLE DOCUMENTS

The contractor shall comply with all documents listed below as mandatory and referenced under
paragraph 4.0, Tasks.

Mandatory compliance:

- Federal Acquisition Regulations (FAR)
- DHS regulations, policies and procedures
- OMB policy and guidance

- Government Accountability Comptroller General Decisions
- Federal fiscal policies
- Applicable Federal, State, and Local Regulations

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 TASK ONE. *Training Support for Procurement Execution*

The contractor will be responsible for assisting in training on DHS and CISA policy including acquisition and contract processes; and content for the monthly acquisition and contract community of practice sessions.

2.1.1 Conduct the COR and PM Community of Practice workshops (COP), meetings and training. The contractor shall assist OCAE conduct monthly meetings with CORs and PMs throughout the Agency. This includes facilation of the meetings; coordination of speakers, setting agendas, producing participant materials and using technology available to meet the needs of staff in virtual environments. Topics are focused on acquisition and contract activities and policies and procedures at the Agency and Headquaters level. Staff who attend are at varied levels of experience and the meetings are reflective of the audience. Staff who attend receive continuous learning points to maintain their certifcations. Audience size can vary from 50-100 people.

2.1.2 Develop contract and acquisition training content and viable interactive instructional delivery methods for staff located virtually and metro DC local. The development of training content will augement the topics covered during ther COP meetings and will be focused on acquisition and contract activities and policies and procedures at the Agency and Headquaters level. Staff who attend are at varied levels of experience and the meetings are reflective of the audience. As requested the CORs and PMs may have topics they wish to see highlighted in the COP meetings and development of associated materials such as briefings, flow charts and information job aides may be needed.

2.2 TASK TWO. *Mature current communities of practice to a self-sustaining capability where monthly meetings can be coordinated and led by operational staff vs senior leadership*

Future COP meetings will be led by government staff and it is expected that the contractor shall document the process for executing meetings. This documentation shall include the use of Sharepoint and associated tools, such as, Poll Everywhere. The contractor is also required to include staff from other areas of the organization, where applicable, in the development and faciltiation process to enhance their knowledge and experience in facilitating COP meetings and developing materials.

2.3 TASK THREE. *Provide organizational and strategic planning for OCAE COCO*

OCAE aspires to improve processes and reduce spending by planning for out year changes in procurement activities. Currently it is the goal of CISA Leadership to combine contracts across the Agency wherever possible and when it makes sense financially without interruption to the Mission. This task includes the analysis of short and long term Agency requirements to develop a strategic roadmap that is actionable over the next 5 years based on the current state of acquisitions and contracts.

2.3.1 Develop strategic plan with actions that can be implemented over the next 5 years, including portfolio analysis review.

2.3.2 Conduct portfolio analysis review.

The contractor shall review the current and planned acquisitions through FY28 to offer recommendations for simplifying, combining or altering current acquisition strategies without disruption to the budget execution year for the Mission.

3.0 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.

3.1 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.

3.2 The COR will have 7 business days to review deliverables and make comments. The Contractor shall have 5 business days to make corrections and redeliver.

3.3 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.

4.0 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	6.7	**Post Award Conference (PAC)**	**Ten business days after award**	**N/A**
2	6.9	**Weekly Progress Meetings**	**Weekly**	**COR, PM**

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
3	6.10	Monthly Progress Reports	Monthly	COR, PM
4	2.2	Host Monthly Community of Practice Meetings, Slide deck and Meeting notes	Monthly	COR, PM
5	2.1	Four instructional design packages	Quarterly	COR, PM
6	2.1, 2.2	Training implementation for key acquisition topics	Quarterly	COR, PM
7	2.1	Design and implement annual half-day CISA-wide acquisition session for entire CISA acquisition workforce.	One time event	COR, PM

5.0 CONTRACTOR PERSONNEL

5.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW.

5.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall ensure that 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 Contracting Officer's Representative (COR) prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

5.3 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. The following Contractor personnel are designated as Key for this requirement. Note: The Government may designate additional Contractor personnel as *Key* at the time of award.

- Senior Project Manager (Oversees all Tasks)

5.3.1 Minimum Qualifications for Key Personnel

Senior Project Manager (All Tasks)

The Senior Project Manager is determined to be a key person under the contract. The Senior Project Manager's duties include oversight of contractor personnel working under this contract and being responsible for all Contractor work performed under this SOW. The Senior Project Manager shall be a single point of contact for the Contracting Officer and the COR. The Senior Project Manager and any designated alternates shall be able to read, write, speak and understand English fluently.

The Senior Project Manager shall be available to the COR via telephone between the hours of 8 and 5 ET, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 24 hours of notification. In the event the Project Manager is not available (e.g., vacation, sick leave, etc.), an alternate shall be identified by the Contractor during his/her absence accompanied by written notification to the COR and shall have all the weight and authority to perform the duties of the Senior Project Manager and act on his behalf. Additionally, the Contractor shall not replace the Senior Project Manager without prior written approval from the Contracting Officer.

- Ability to obtain and/or possess suitability determination

  - MA/MS degree preferred. An additional five (5) years of relevant experience may be substituted for the MA/MS degree.
  - Minimum of Fifteen (15) years of demonstrated experience supporting requirements of the same size and scope.

5.4 Minimum Qualifications for Non-Key Personnel

5.4.1 Senior Management Consultant (All Tasks):

- Ability to obtain and/or possess suitability determination

  - MA/MS degree preferred. An additional five (5) years of relevant experience may be substituted for the MA/MS degree.
  - Minimum Fifteen (15) years' experience in the following:
    - Leading change initiatives or projects involving broad, large-scale changes in the organizational structure and job roles of a public sector organization, as well as changes in business processes
    - Possesses requisite knowledge of organizational design and change management theory, methodologies, and best practices
    - Leading development of strategies and plans to move organizations forward in implementing organization-wide changes
    - Leading engagement with a workforce represented by multiple unions distributed across the Nation.
    - Providing customized business-focused objective advice, expertise, and specialist skills to create value and improve business strategy, internal processes and program/project performance
    - Providing advice directly for executive-level consumption
    - Leading, devising and implementing goals, objectives, milestones, and performance measures to assess an organization's success in implementing change

- Maintaining responsibility for managing business solutions, delegating appropriate resources, and fostering quality assurance principles across projects and deliverables and resolving issues
- Overseeing process and productivity improvement, systems alignment, organizational assessments, and program audits and evaluations

5.4.2 **Management Analyst (Tasks 2.1, 2.2, & 2.3)**

- Ability to obtain and/or possess favorable DHS fitness determination.
- BA/BS degree. An additional two (3) years of relevant experience may be substituted for the BA/BS degree.
- Minimum seven (7) years' experience in the following:
  - Developing and conducting complex qualitative and quantitative studies, research and analysis to evaluate, integrate or improve program/project productivity
  - Identifying and developing methods, plans, and documentation to streamline operating procedures, reports and systems to improve operations, achieve savings, and encourage long-range planning to assure the program/project produce results in a cost effective manner.

5.4.3 **Jr. Research Data Analyst (Task 2.2 & 2.3)**

- Ability to obtain and/or possess favorable DHS fitness determination.
- AA/AS degree. An additional two (2) years of relevant experience may be substituted for the AA/AS degree.
- Minimum five (5) years' experience in the following:
  - Applies extensive knowledge and experience to obtain, integrate and report client data; develops and applies analytic methodologies and principles
  - Leads the application of analytic techniques and helps define project objectives and strategic direction
  - Resolves complex problems, which require an in-depth knowledge of analytic methodologies and principles
  - Analyzes acquisition data, formulates conclusions and recommendations, designs and develops materials, and evaluates effectiveness in accordance with stated guidelines, specifications, and models
  - Conducts research, data gathering, and technical reviews.
  - Produces written deliverables to include reports, spreadsheets, databases, formal process mapping, technical design, system testing and implementation activities
  - Troubleshoot issues in reports related to data
  - Assimilates, integrates, and interfaces technical knowledge with business / systems requirements

5.5 Employee Identification

5.5.1 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 not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

5.5.2 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 display the Government issued badge in plain view above the waist at all times.

5.4 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 present a professional appearance at all times 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.

5.5 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer*), 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.

6.0 OTHER APPLICABLE CONDITIONS

6.1 PERIOD OF PERFORMANCE

The period of performance for this contract is a one-year base period with two one-year option periods as follows:

Base Period	*August 18, 2024 through August 17, 2025*
Option Period One	*August 18, 2025 through August 17, 2026*

6.2 PLACE OF PERFORMANCE

The primary place of performance will be the Contractor's facilities with frequent visits to the Department of Homeland Security facilities in the Washington Metro Area.

6.3 CONTRACTOR TELECOMMUTING – REMOTE PERSONAL RESIDENCE WORK LOCATIONS.

Telecommuting for federal government contractors will be considered on a situational basis to the extent practicable to meet DHS mission needs. Telecommuting allows contractor personnel to perform their contractual requirements outside of CISA office locations, typically at a contractor's personal residence or a corporate telecommuting office location. Telecommuting for contractor personnel provides the government flexibility to meet unique CISA organizational and facility needs and requirements. The goal of telecommuting for contractor personnel is to enhance the delivery of services that support the DHS mission. Telecommuting is permitted under the task order in accordance with the requirements below.

Additionally, the provision to permit contractor telecommuting may be revoked at the Task Order level at any time if the Government makes such determination. The telecommuting provision does not change any task order requirements; all other terms and conditions of the task order remain in full force and effect.

6.4 CONTRACTOR LABOR RATES CHARGED WHILE TELECOMMUTING

The contractor shall charge the same applicable fixed hourly rate as for a Government site for those contractor personnel when they telecommute at their designated telecommuting location.

6.5 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 8:00 and 4:30 EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW.

6.6 TRAVEL

Contractor travel shall not be required for this requirement.

6.7 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 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 via teleconference.

6.9 PROGRESS REPORTS

The Project Manager shall provide a monthly progress report to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

6.10 PROGRESS MEETINGS

The Project Manager shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place via teleconference.

6.12 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 XP and Microsoft Office Applications).

7.0 GOVERNMENT TERMS & DEFINITIONS

5.1 COR – Contracting Officer's Representative
5.2 DHS – Department of Homeland Security
5.3 CISA – CyberSecurity InfrasturctureSecurity Agency
5.4 OCAE – Office of Chief Acquisition Executive
5.5 COCO- Chief Office of Contracting Official
5.6 PM- Project Manager

5.7 COP- Community of Practice

8.0 GOVERNMENT FURNISHED RESOURCES

The Government will provide the following property to the Contractor for work required under this contract:

Government Furnished Equipment
Laptop

The Government will provide the following equipment for off-site Contractor use in performing work under this contract:

Government Furnished Equipment

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.

8.1 Property Inventory

Contractor/Servicing Agency must establish and maintain an accurate master inventory of all property purchase for CISA under this Contract.

8.2 Monthly Asset Management Report

Contractor/Servicing Agency will ensure personnel prepare a monthly Asset Management Report, which contains accurate information for all CISA property located at their facility. At a minimum, this report must include:

- DHS Barcode
- Acquisition Date
- Acquisition Status
- Asset Condition
- Manufacturer Name
- Manufacturer Model
- Asset Description
- Serial Number
- Asset Cost
- Location

9.0 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 SOW 2.0 and SOW 6.0, 8.0

9.1 Property Inventory

The Contractor/Servicing Agency will ensure personnel apply a DHS-supplied barcode to all property purchased for CISA. Contractor/Servicing Agency must establish and maintain an accurate master inventory of all property purchase for CISA under this Contract.

10.0 Monthly Asset Management Report

Contractor/Servicing Agency will prepare a monthly Asset Management Report, which contains accurate information for all CISA property located at their facility. At a minimum, this report must include:

- DHS Barcode
- Acquisition Date
- Acquisition Status
- Asset Condition
- Manufacturer Name
- Manufacturer Model
- Asset Description
- Serial Number
- Asset Cost
- Location

10.1 Invoice/Receipts

Contractor/Servicing Agency will ensure copies of all invoices/packing slips/receipts for property purchased for CISA accompanies the Monthly Asset Management Report.

11.0 INVOICES AND PAYMENT PROVISIONS

Invoices shall be prepared per Section VII, Contract Clauses; Paragraph A. entitled "FAR CLAUSES INCORPORATED BY REFERENCE," FAR Clause 52.232-25 Prompt Payment. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

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

The contractor shall submit invoices monthly. The Contractor shall submit the invoice electronically to the address below:

E-mail: [redacted]

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

[redacted]

The contractor shall submit invoices to the email addresses above. Additionally, the contractor shall prepare and submit a sufficient and procurement regulatory compliant invoice and receiving report for technical certification of inspection/acceptance of services and approval for

payment. The contractor shall attach back up information to the invoices and receiving reports substantiating all costs for services performed. The receiving agency's written or electronic acceptance by the COR and date of acceptance shall be included as part of the backup documentation.

If the invoice is submitted without all required back up documentation, the invoice shall be rejected. The Government reserves the right to have all invoices and backup documentation reviewed by the Contracting Officer prior to payment approval.

12.0 RECORDS MANAGEMENT OBLIGATIONS

12.1 Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

12.2 In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

12.3 In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

12.4 CISA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of CISA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to CISA. The agency must report promptly to NARA in accordance with 36 CFR 1230.

12.5 The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the [contract vehicle]. The

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

12.6 The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and CISA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

12.7 The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with CISA policy.

12.8 The Contractor shall not create or maintain any records containing any non-public CISA information that are not specifically tied to or authorized by the contract.

12.9 The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

12.10 CISA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which CISA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

12.11 Training

All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take CISA-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

12.12 Flowdown of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract vehicle, if applicable, and require written subcontractor acknowledgment of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

13.0 SECURITY

Contractor will NOT have access to unclassified, but Security Sensitive Information may be required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS

The procedures outlined below shall be followed for the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD) to process background investigations, Entry on Duty determinations, and Fitness determinations, as required, in a timely and efficient manner.

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

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS OCSO/PSD. Prospective contractor employees shall submit the below completed forms to the DHS OCSO/PSD. The Standard Form (SF) 85-P must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85P signature pages and other completed forms must be given to the OSCO/PSD no less than thirty (30) days before the start date of the contract or thirty (30) days prior to the requested entry on duty date, for all contractor employees whether a replacement, addition, subcontractor employee, or vendor:

Standard Form (SF) 85-P, —Questionnaire for Public Trust Positions‖
SF-85P Certification
SF-85P Authorization for Release of Information
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 Reports Pursuant to the Fair Credit Reporting Act

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

The DHS OCSO/PSD may, as it deems appropriate, authorize and grant a favorable Entry on Duty (EOD) decision based on preliminary checks. A favorable EOD decision allows a contractor employee to commence work temporarily prior to the completion of

the full background investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable Fitness determination will follow. In addition, a favorable EOD or Fitness determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD or Fitness determination by the DHS OCSO/PSD.

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

The DHS OCSO/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer's Representative (COR) all DHS issued 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 whom it was issued and the last known location and disposition of the pass or card.

13.1 PROTECTION OF INFORMATION

The Government will provide all necessary information, data and documents to the Contractor for work required under this contract.

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.

REFERENCES:
DHS Management Directive 140-01, "*Information Technology System Security Program, Sensitive Systems*"

- DHS 4300A Policy Directive (Version 13.3, February 13, 2023).
- DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018 for NSS Collateral (Unclass, Secret or Top Secret Collateral).
- DHS Sensitive Compartmented Information (SCI) Systems 4300C Instruction Manual, Version 2.1, March 24, 2017 for TS SCI/C-LAN.

1. DHS and CISA ENTERPRISE ARCHITECTURE COMPLIANCE

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

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical

Reference Model (TRM) Standards and Products Profile.

- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the CISA Chief Data Officer 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 CISA's Enterprise Data Management Program Policy and all data-related artifacts will be developed and validated according to DHS and CISA 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.

2. DHS GEOSPATIAL INFORMATION SYSTEM TERMS AND CONDITIONS

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

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

3. EPEAT AND ENERGY STAR LANGUAGE

All hardware procured directly or in support of this action must meet applicable and appropriate Electronic Product Environmental Assessment Tool (EPEAT) and ENERGY Star standards.

4. DHS CYBER-SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) TERMS & CONDITIONS

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.

5. SECTION 508 REQUIREMENTS

Section 508 applicability to Information and Communications Technology (ICT): Web and Non Web Based Electronic Deliverables

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

Applicable Functional Performance Criteria: Does not apply

Applicable 508 requirements for electronic content features and components (including but not limited to Electronic documents; Electronic forms; Electronic document templates; Electronic surveys; Electronic reports; Electronic training materials): All requirements in E205 apply, including all WCAG 2.0 Level A and AA Success Criteria apply as specified in E205

Applicable 508 requirements for software features and components: Does not apply

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

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

Section 508 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.

6. THE HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12)

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

- The DHS 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 Personal Identity Verification (PIV) credentials/identification cards and building passes that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or card."

7. ARTIFICIAL INTELLIGENCE/MACHINE LEARNING REQUIREMENTS

Definitions: Artificial Intelligence (AI) includes the following: (1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks. (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task. (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

Requirements:
The 2019 National Defense Authorization Act (NDAA) and Executive Order (EO) 13960 require that AI used in the Federal Government foster public trust and confidence while protecting privacy, civil rights, civil liberties, and American values. All federal employees, contractors, and subcontractors, when designing, developing, acquiring, and/or using AI for or within DHS, will adhere to the following 9 principles.

1. Lawful and respectful of our Nation's values: Agencies shall design, develop, acquire, and use AI in a manner that exhibits due respect for our Nation's values and

is consistent with the Constitution and all other applicable laws and policies, including those addressing privacy, civil rights, and civil liberties.

2. Purposeful and performance-driven: Agencies shall seek opportunities for designing, developing, acquiring, and using AI, where the benefits of doing so significantly outweigh the risks, and the risks can be assessed and managed.
3. Accurate, reliable, and effective: Agencies shall ensure that their application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective.

4. Safe, secure, and resilient: Agencies shall ensure the safety, security, and resiliency of their AI applications, including resilience when confronted with systematic vulnerabilities, adversarial manipulation, and other malicious exploitation.

5. Understandable: Agencies shall ensure that the operations and outcomes of their AI applications are sufficiently understandable by subject matter experts, users, and others, as appropriate.

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

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

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

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