TASK ORDER 02

STATEMENT OF WORK (SOW) FOR
Strategic Workforce Operations and Specialized Project Management Support

Revision 1

1.0 GENERAL

1.1 BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA), Cybersecurity Division (CSD), Vulnerability Management (VM) Sub-Division brings together cyber vulnerability focused teams from across the CSD to reduce the attack surface of government and critical infrastructure and enable customers and stakeholders to make data-driven decisions to manage their own risk portfolios. VM's mission is to reduce risk to the Nation by assisting and enabling stakeholders to understand and manage vulnerabilities. Five strategic goals support this mission:

1. Reduce Stakeholder Vulnerabilities
2. Increase National Resilience
3. Enable Data-Driven Decisions
4. Influence Operational Behaviors
5. Promote and Support the Responsible Disclosure of Vulnerabilities.

CISA with practical, first-hand awareness and understanding of the operational risks present in national critical systems and functions. Leveraging these insights, CISA champions and promotes data-driven and defensible policies, strategies and initiatives tailored to address the most urgent vulnerabilities, reducing risk, and increasing national resilience. VM's responsible disclosure activities build trust with the public and our stakeholders and provide the basis for normalized, coordinated, and collaborative disclosure of identified vulnerabilities worldwide.

1.2 SCOPE

This action is to procure specialized and experienced services to provide the VM sub-division with strategic workforce operations and budgetary support to include assisting federal employees with the oversight and management of sub-division expenses and identifying any financial risks within the yearly program budget by maintaining and tracking financial data and program expenditures.

1.3 OBJECTIVE

The objective is to staff VM with knowledgeable experts in employee engagement and strategic workforce operations to enable the continued growth of VM and to meet the following cultural objectives as defined by VM leadership:

- Always assume good intent
- Always work to maximize stakeholders across the organization
- Aim to overcommunicate

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 TASK ONE: PROGRAM MANAGEMENT

2.1.1. Contract Management
The Contractor shall submit a draft Program Management Plan (PMP) describing the technical approach, organizational resources, and management controls to be employed to meet the performance and schedule requirements throughout the execution of each task area described below. The PMP shall include productivity and management methods such as quality assurance, methods for detailed progress/status reporting and program reviews, and shall indicate the provision of centralized administration and clerical, documentation, and related functions. The Contractor shall prepare and present Monthly Status Reports (MSRs), which address the progress/status of each of the tasks described below, including quality assurance information, any changes made in the PMP, and serve as the vehicle that establishes firm dates for deliverables. Within the MSRs, the Contractor shall provide the following information:

- An overview of work completed, in progress, and planned for each task.
- Identification of problem areas with recommended remedial actions.
- Summary of resource expenditures.
- Status of all issues identified during the course of the last review.

2.1.2 Contract Kickoff

The Contractor shall attend a kickoff meeting with the Contracting Officer and the Contracting Officer's Representative (COR) within ten business days of Task Order award unless directed otherwise by the Government. The purpose of the Kickoff meeting, which will be chaired by the CO or COR, is to discuss technical and contracting objectives of this Task Order. The Kickoff meeting will be held at the Government's facility or via Microsoft Teams. The Contractor shall submit the Kickoff Briefing at this meeting.

The Contractor shall develop a proposed kickoff meeting agenda within ten business days after award of this Task Order. The Contractor shall deliver an electronic copy to the COR at least two calendar days before the scheduled kickoff meeting. The Contractor shall document the minutes and action items from the Kickoff meeting.

The draft PMP shall be due 30 days after the date of the Kickoff meeting.

2.1.3 Staffing Plan

The Contractor shall submit a staffing plan at the initiation of the contract. The Contractor shall update the plan for each Monthly Status Report at a minimum to identify and properly track all staff working on the Task Order. The COR may require weekly updates at Task Order initiation in order to track hiring and onboarding progress to include equipment distribution.

2.2 TASK TWO. Workforce Operations Program Development and Execution (Human Capital & Employee Engagement)

2.2.1 Workforce Operations Human Capital Plan Development

The Contractor shall develop through coordination with VM Leadership and VM Workforce Operations a Human Capital Liaison plan that describes all of the task/processes necessary to manage the human capital activities for VM. This plan will include various reporting mechanisms that will be used to quickly and efficiently gather historical and future human capital

data for VM.

2.2.2 Workforce Operations Human Capital Plan Maintenance

The Contractor shall provide ongoing maintenance to the Workforce Operations Human Capital Plan. This plan is developed annually; however, changes over the course of the fiscal year will require out of cycle adjustments to the plan for it to remain accurate and up to date. The plan will continue to evolve to align with the workforce and organizational processes that are fluid and likely to change based on emerging requirements. Therefore, the Contractor shall conduct periodic reviews and updates of the Workforce Operations Human Capital Plan to ensure that it continues to be in alignment with the VM operational mission and meets Agency and Division requirements.

2.2.3 Human Capital Liaison Execution

The Contractor shall support the execution of tasks and deliverables described in the VM Workforce Operations Human Capital Plan. The Contractor shall provide support by serving as a liaison between the CISA Human Resource office, VM hiring managers and CSD Front Office. Examples of supported activities could include, but not be limited to:

- Table of Organization Change Request
- Position Description Classification
- OPM Request for Vacancy Announcement
- Job Fair Packets
- Tracking/Managing VM's vacant/filled billets
- Daily Human Capital Reporting

2.2.4. Workforce Operations Annual Employee Engagement Plan Development

The Contractor shall develop through coordination with VM Leadership and VM Workforce Operations an annual Employee Engagement Plan that describes all of the events or activities over the course of a to-be-defined 12-month cycle (e.g. fiscal year or calendar year) that will accomplish the goals of VM Workforce Operations. These events and activities can include, but are not limited to orientations, brown bag informational sessions, leadership training events, and all hands meetings.

2.2.5 Employee Engagement Plan Execution

The Contractor shall support the execution of the projects described in the VM Workforce Operations Annual Employee Engagement Plan. Examples could include, but not be limited to:

- Provide support of VM All-Hands meetings
- Planning and Execution of Team Building Activities at the VM or VM-branch level
- Logistical Support for VM offsite meetings
- Operations and Maintenance of the VM Orientation Program
- Facilitation of internal training/brown bag meetings
- Development and Implementation of VM Internal Awards program
- Provide support for VM's participating in CISA and CSD Award programs

2.2.6 Employee Engagement and Knowledge Management Execution

The Contractor shall provide support to the VM Knowledge Management team, contribute to the growth and refinement of the VM Knowledge Management repository as required. They would

also help to facilitate and execute collaborative efforts across VM to find optimal solutions to find, store, display, and automate relevant information, content, and processes; both external to VM as well as internally to each branch within VM in order to maximize employee engagement with VM informational systems. The Contractor shall have a high degree of familiarity with tools such as, but not limited to, ServiceNow, SharePoint, and O365.

2.3 TASK THREE. Specialized Project Management Support

The Contractor shall provide ongoing project management support to VM in the following specialized area:

2.3.1 Budgetary Support

The Contractor shall provide subject matter expertise to support governmental management of budgetary requirements across the VM Sub-Division. The objective of budgetary management is to provide the oversight and management of sub-division project expenses while at the same time, helping to identify any financial risks. The Contractor shall work with VM sub-division project managers to help them measure and track variances from their cost baselines and advise them on corrective actions when necessary. The Contractor shall also support the development and execution of a VM budget change control process.

3.0 CONTRACTOR PERSONNEL

3.1 Key Personnel

Before replacing any individual designated as Key by the Government, the Contractor shall notify the Contracting Officer no less than fifteen 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 written approval from the Contracting Officer.

The following Contractor personnel are designated as Key for this contract.

1. Program Manager (PM)

The PM shall possess the following core competencies:

- Ability to provide overall strategic management and manages project's scope, schedule, budget, and risk.
- Reviews risk and risk mitigation activities of the program and proposes budgets for the same.
- Coordinates schedules to facilitate completion of task and contract deliverables, briefings/presentations, and program reviews.
- Knowledge of ensuring adherence to quality standards and reviews program deliverables.
- Develops detailed work plans, schedules, project estimates, resource plans, and status reports for assigned programs with minimal guidance.
- Conducts program meetings and is responsible for program tracking and analysis.
- Recommends and takes action to direct the analysis and solutions of problems.

In addition to the core competencies above, the PM shall possess the following:

- 4-6 years project management experience on Federal programs

The PM position is not estimated to require a full time FTE. The Contractor can either provide a part time PM or have the PM function be filled concurrently by someone on the Task Order under another labor category.

3.2.1 The PM shall be available to the COR via telephone between the hours of 0900 and 1600 ET, Monday through Friday, and shall respond to a request for discussion or resolution of problems within 24 hours of notification.

3.3 Employee Identification

3.3.1 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.

3.3.2 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.

3.4 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 PM shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

3.5 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.

4.0 OTHER APPLICABLE CONDITIONS

4.1 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.

4.1.1. Requests for Exception to U.S. Citizenship Requirement

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

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

4.2.2. 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 Task 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 each individual will perform on the Task Order. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigation s 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

Reports 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 Task Order.
- 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. No employee of the Contractor shall be allowed to EOD and/or access sensitive information or systems without a favorable EOD decision or suitability determination.
- 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'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 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 or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).
    - Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.

4.2 Security Compliance

All services provided under this Task Order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

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 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 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.

DHS 4300A Policy 3.3 Contractors and Outsourced Operations
DHS 4300A Policy - 3.3.b. All Contractor information system services and operations shall adhere to all applicable DHS information security policies.

DHS 4300A Policy 3.12 Information Security Policy Violation and Disciplinary Action
DHS 4300A Policy - 3.12.b. Non-DHS Federal employees, contractors, or others working on behalf of DHS who fail to comply with Department security policies are subject to termination of their access to DHS systems and facilities whether or not the failure results in criminal prosecution.

DHS 4300A Policy 4.2.1 General Physical Access
DHS 4300A Policy 4.2.1.d - Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.

DHS 4300A Policy 5.5.1 Encryption
DHS 4300A Policy - 5.5.1.a Systems requiring encryption shall comply with the following methods: Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2 National Security Agency (NSA) Type 2 or Type 1 encryption (Note: The use of triple Data Encryption Standard [3DES] and FIPS 140-1 is no longer permitted.)

DHS 4300a Policy - 5.5.1.b Components shall develop and maintain encryption plans for sensitive information systems.

DHS 4300a Policy - 5.5.1.c Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use.

4.3 PERIOD OF PERFORMANCE

The period of performance for this Task Order is 9/1/2024 – 8/31/2025.

4.4 PLACE OF PERFORMANCE

The Contractor shall perform work at the DHS facility located at 1110 North Glebe Road, Arlington VA 22201, other DHS offices located in the Washington, DC metropolitan area or at Contractor facilities as required by the government. During performance under this contract, Contractor personnel shall be available at a minimum during core business hours of 9:00 am to 3:00 pm eastern time. Specific work schedules for personnel working onsite shall be coordinated with the COR.

VM promotes telecommuting for Federal Government contractors to the greatest extent possible to meet mission needs. Telecommuting allows contractor personnel to perform their contractual requirements outside of VM 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 VM organizational and facility needs and requirements. The goal of telecommuting for contractor personnel is to enhance the delivery of services that support the VM mission. Telecommuting is permitted under this Contract in accordance with the requirements below. The provision to permit Contractor telecommuting may be revoked at any time if the Government makes the determination that it is in the best interests of the Government to do so or changing missions requirements require it.

- Requests for telework must be submitted by the Contractor's PM to the COR, prior to telework beginning.
- At any time, the COR shall revoke the telework privilege for a particular individual as long as sufficient workspace is available at the Government or Contractor work site.
- The Contractor shall charge the same applicable fixed hourly rate (whether Contractor or Government site) for the Contractor personnel when they telecommute at their designated telecommuting location.

4.5 HOURS OF OPERATION

Contractor employees shall perform work during core hours Monday through Friday (except Federal holidays). During performance under this contract, Contractor personnel shall be available at a minimum during core business hours of 9:00 am to 3:00 pm eastern time. 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. When work or travel is required to be completed during holidays or weekends the vendor will submit a written request for the COR to be approved based on mission requirements.

4.6 TRAVEL

Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

4.7 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).

4.8 INTELLECTUAL PROPERTY

No data provided to, or developed by, the Contractor shall be used for any purpose other than in support of, or as designated by, CISA. All information (data files, hard copies, other electronic or paper documents, etc.) shall be in accordance with FAR 52-227-14 Rights in Data-General. All products that the Contractor may develop under this contract shall be in accordance with FAR 52- 227-14 Rights in Data-General.

4.9 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.

Contractor access to information protected under the Privacy Act is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

Contractor access to proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

4.10 RECORDS MANAGEMENT OBLIGATIONS

4.10.1 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.

4.10.2 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.

4.10.3 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.

4.10.4 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.

4.10.5 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. 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. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

4.10.6 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 requiring0 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.

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

4.10.8 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.

4.10.9 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.

4.10.10 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.

4.10.11 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.

4.10.12 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 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.

5.0 GOVERNMENT TERMS & DEFINITIONS

COR	Contracting Officer's Representative
DHS	Department of Homeland Security
SOW	Statement of Work
CSD	Cybersecurity Division
VM	Vulnerability Management
CISA	Cybersecurity and Infrastructure Security Agency
SOP	Standard Operating Procedure
PM	Project Manager
PII	Personally Identifiable Information
PCII	Protected Critical Infrastructure Information

6.0 GOVERNMENT FURNISHED RESOURCES

The Contractor might use Government furnished facilities, property, equipment and supplies for the performance of work under this Task Order. The Contractor 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 for the performance of work under this Task Order 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.

7.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this Task Order, except for the Government Furnished Resources specified in SOW 6.0.

8.0 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	2.1.2	Post Award Conference	NLT 10 business days after contract award	N/A
2	*2.1.1*	*Draft Program Management Plan*	*NLT 30 business after Post Award Conference*	*COR, Contracting Officer*
3	***2.1.1; 2.1.3***	***Monthly Status Reports; Staffing Update***	***Monthly***	***COR, Contracting Officer; Federal Task Leads***
4	2.2.1	Workforce Operations Human Capital Plan - Draft	90 days after contract award	COR, Contracting Officer, Workforce Operations Task Lead
5	2.2.1	Workforce Operations Human Capital Plan – Final	120 days after contract award	COR, Contracting Officer, Workforce Operations Task Lead
6	2.2.2	Workforce Operations Human Capital Plan Maintenance	Ongoing	N/A
7	2.2.4	Employee Engagement Plan	90 days after contract award	Contracting Officer, Workforce Operations Task Lead
8	2.2.5	Employee Engagement Plan Execution	Ongoing	N/A

9.0 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.

9.1 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.

9.2 The COR will have ten business days to review deliverables and make comments. The Contractor shall have five business days to make corrections and redeliver.

9.3 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.