DEPARTMENT OF HOMELAND SECURITY (DHS)

STATEMENT OF WORK (SOW)
FOR
FEDERAL EMPLOYEE VIEWPOINT SURVEY (FEVS) DATA ANALYSIS AND ACTION PLANNING

1.0 GENERAL

1.1 BACKGROUND

The Office of Cybersecurity and Infrastructure Security (CISA) mission is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. CISA is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. CISA actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm strategic assets.

CISA works to prevent or minimize disruptions to our critical information infrastructure in order to protect the public, the economy, government services, and the overall security of the United States. It does this by supporting a series of continuous efforts designed to further safeguard federal government systems by reducing potential vulnerabilities, protecting against cyber intrusions, anticipating future threats, enhancing the security and reliability of the cyber ecosystem, and ensuring the interoperability and continuity of national security and emergency preparedness communications.

The CISA consists of the following divisions:

- Cybersecurity Division (CSD)
- Emergency Communications Division (ECD)
- Integrated Operations Division (IOD)
- Infrastructure Security Division (ISD)
- Stakeholder Engagement Division (SED)
- Enterprise Performance Management Office
- National Risk Management Center (NRMC)

The NRMC is headquartered with the National Capital Region (NCR).

1.2 SCOPE

The contractor shall provide employee engagement support services for the accomplishment of CISA core values. Specifically, the scope shall focus on the following areas:

- Conduct an analysis of the 2024 Federal Employee Viewpoint Survey (FEVS) results for NRMC
- Conduct NRMC employee focus groups and surveys to understand the specific root-cause of workforce issues. Qualitative data collection shall focus on key issues identified on the FEVS results and other issues identified by CISA and NRMC senior leadership.
- Develop action plans to resolve employee pain points identified on data analysis and

focus groups results to improve employee engagement.
- Assist NRMC in implementing solutions to address employee pain points.

1.3 OBJECTIVE
The objective is to be able to develop a data based, action plan in order to develop an efficient and effective response to the FEVS survey results.

1.4 APPLICABLE DOCUMENTS

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

a) DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27. 2017
b) DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2028

1.4.2 Reference Documents
The following documents may be helpful to the Contractor in performing the work described in this document:

a) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified Information
b) Department of Homeland Security Suitability and Fitness Program, Instruction Handbook Number 121-01-011, Department of Homeland Security Administrative Security Program
c) DHS Privacy Policy Guidance Memorandum 2011-02 Roles and Responsibilities for Shared IT Services

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 TASK ONE. FEVS ANALYSIS AND ACTION PLANNING

Contractor shall conduct an analysis of the results from the 2024 Federal Employee Viewpoint Survey (FEVS) for National Risk Management Center (a total of approximately 140 employees may be eligible to respond to the survey). This assessment shall identity the key issues impacting employee engagement at CISA. The contractor shall conduct a comparative analysis of NRMC FEVS data with the CISA FEVS results. The quantitative analysis shall include a review and subsequent explanation of the results for each question, as well as a roll-up or summary of the results for each FEVS section. These results shall be benchmarked against CISA results to illustrate how NRMC performed against each question and category relative to other CISA Divisions / Mission Enabling Offices. Additionally, the contractor shall complete briefing materials that translate the quantitative data into understandable terms and visual graphics, to be presented by NRMC Senior Leadership to the NRMC workforce. The contractor shall identify three (3) primary areas of interest for focus group and action planning, based on the results. These areas of interest shall be those which suggest pain points or areas of

concern widely shared across the workforce, or particularly mis-aligned with other CISA Division/MEO results.

The Contractor shall develop the following deliverables for this task:

1. Qualitative analysis report
2. Briefing book with talking points for presentation to NRMC workforce
3. Identification of three areas of interest for focus grouping

2.2 TASK TWO. FOCUS GROUPS

The contractor shall be responsible for planning all the logistics of the focus groups, such as planning meeting times, locations, facilitation, and note taking. The contractor shall coordinate with the Government Program Manager for focus schedule, duration, scope, questions. The contractor shall coordinate with the government Program Manager if additional surveys will be conducted in addition to focus groups. Additional surveys will be required if the results of the data analysis and focus groups demonstrate a need to do so.

The contractor shall facilitate three (3) focus groups with respondents and NRMC employees to identify areas relevant to FEVS results which could be improved to enhance the employee experience, based on FEVS and action planning feedback. This task includes developing the focus group plan (how many, structure, primary topic areas); creating the focus group facilitation materials; scheduling the focus groups, including soliciting participation from NRMC workforce; facilitating the focus groups (virtual environment; 1 to 2 hours each); taking notes and recording observations from each focus group; and delivering a complete report of results after the completion of all focus groups. The objective for the focus groups will be to target specific areas relevant to the FEVS results and understand root causes and potential resolutions or opportunities for improvement.

The contractor shall develop the following deliverables for this task:

1. Focus group project plan
2. Focus group facilitation materials (briefing, intent/objective, interview questions, leading questions, group exercises)
3. Focus group minutes and key observations
4. Summary report of focus group findings

2.3 TASK THREE. DEVELOP ACTION PLANS

The contractor shall develop action plans that address identified areas for improvement based on focus groups' feedback. NRMC will assist in identifying which focus group findings will require an action plan. The contractor shall develop Action Plans that map to specific feedback from the FEVS survey, as well as Focus Group results. The contractor shall develop five (5) 0) action plans are requested. Each Action Plan shall be discrete and include an action-based statement and goal/objective. The Action Plan shall also utilize data analysis and focus group results to develop strategies to hire and retain the best and brightest employees by identifying resources employees required to perform their jobs, training requirements, and career development tools/strategies necessary to meet their needs. Each action plan shall clearly state:

1. Which question or category the action plan most closely aligns to from the FEVS survey?
2. Which results or feedback from Focus Grouping relates most closely to the Action Plan?
3. What the FEVS and Focus Groups insights are with regard to the Action Plan topic?
4. What the Action Plan aims to achieve?
5. Specific action-oriented statements with goals and suggestions for implementation.

2.4 TASK FOUR. IMPLEMENT ACTION PLANS

Upon completion of Tasks 2.1 to 2.3, the contractor shall assist the Government in facilitating and implementing the selected recommendations to resolve employee pain points identified in the data analysis, focus groups and/or surveys. The contractor shall assist in implementation of targeted action plan areas, including but not limited to tracking actions, developing employee communications, providing automated tools, delivering training/brown bag materials, and authoring processes or policies that will address relevant topic areas.

When requested, the contractor shall assist in implementing action plans. This may include, but is not limited to, deliverables such as:

- Standard Operating Procedure development
- Workflow Visualizations
- Development of Employee Engagement or Internal Communication materials
- Delivery of and/or Development of Brown Bag Materials
- SharePoint site development

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 shall 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 ten (10) business days to review deliverables and make comments. The Contractor shall have five (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	2.1	**Qualitative Analysis Report**	30 Days after FEVS results are issued	PM, COR
2	2.1	**Briefing Book with talking points for presentation to NRMC workforce**	30 Days after FEVS results are issued	PM, COR
3	2.1	**Identification of three (3) areas of interest for focus grouping**	45 Days after FEVS results are issued	PM, COR
4	2.2	**Focus group project plan**	45 Days after FEVS results are issued	PM, COR
5	2.2	**Focus group facilitation materials**	45 Days after FEVS results are issued	PM, COR
6	2.2	**Focus group minutes and key observations**	5 Days after Focus Group	PM, COR
7	2.2	**Summary report of focus group findings**	5 Days after focus group	PM, COR
8	2.3	**Five Action Plans addressing Key Findings from Focus Group.**	21 Business Days after last Focus Group	PM, COR
9	2.4	*Ad Hoc Implementation Materials*	TBD	PM, COR
10	6.8	**Draft Project Plan with proposed timing and milestones.**	At Post Award Conference	PM, COR
11	6.8	**Final Project Plan with proposed timing and milestones.**	30 Days after Post Award Conference	PM, COR, Contracting Officer
12	11.0	**Invoices**	Monthly	PM, COR, Contracting Officer

5.0 CONTRACTOR PERSONNEL

The Contractor shall fill vacancies with contract personnel who are skilled, trained, and qualified to support specific job functions as described within the SOW. Contractor support personnel shall conduct themselves professionally and maintain a professional demeanor when interacting with Government employees, agencies, or offices.

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.

The Key Personnel or Facilities under this Contract:
Senior Program Manager

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

5.4 Senior Program Manager

The Contractor shall provide a Senior Program Manager who shall be responsible for all Contractor work performed under this SOW. The Senior Program Manager shall be a single point of contact for the Contracting Officer and the COR. It is anticipated that the Senior Program Manager shall be one of the senior level employees provided by the Contractor for this work effort. The name of the Senior Program Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Senior Program Manager, shall be provided to the Government as part of the Contractor's proposal.

The Senior Program Manager is further designated as *Key* by the Government. During any absence of the Senior Program Manager, only one alternate shall have full authority to act for

the Contractor on all matters relating to work performed under this contract. The Senior Program Manager and all designated alternates shall be able to read, write, speak and understand English. Additionally, the Contractor shall not replace the Senior Program Manager without prior approval from the Contracting Officer.

The Senior Program Manager shall:

- have experience managing Programs relating to private and public sector information sharing and leading teams working in a fast-paced environment with private and/or federal sector stakeholders.

- have developed and implemented process methodologies at an agency or corporate level for analytic programs.

- have at least ten (10) years of experience and a MA/MS degree or higher or fifteen (15) years of experience with a college degree.

5.4.1 The Senior Program Manager shall be available to the COR via telephone between the hours of 8:00 AM and 5:00 PM EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 24 hours of notification.

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.

5.5 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 Senior Program Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

5.6 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 one year from the date of award.

6.2 PLACE OF PERFORMANCE

The place of performance will be at the Contractor's facility or contractor approved location. .

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.

Contractor and/or subcontractor employees shall not telecommute on Federal holidays, other non-workdays, or in the case of a pandemic or other emergency or unforeseen situation such as an epidemic, natural disaster, early closing or delayed opening of the Government, as well as a Government shutdown without prior written approval of the COR.

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 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 8:00 AM and 5:00 PM EST, Monday through Friday (except Federal holidays).

Services will generally not be required on the following Federal holidays (or any other holidays declared by the Government); however, the Contractor may be required to provide services on these days in support of mission critical situations.

- New Year's Day – 1 January
- Martin Luther King's Birthday - Third Monday in January
- Inauguration Day – January 20 (or 21st if the 20th is a Sunday)
- Washington's Birthday - Third Monday in February
- Memorial Day - Last Monday in May

- Juneteenth National Independence Day – 19 June
- Independence Day - 4 July
- Labor Day - First Monday in September
- Columbus Day - Second Monday in October
- Veterans Day - 11 November (or as observed)
- Thanksgiving Day - 4th Thursday in November
- Christmas Day - 25 December

6.5 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 five (5) 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 at the Government's facility, located at [redacted] or via teleconference.

6.8 PROJECT PLAN

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 thirty (30) business days after the Post Award Conference.

6.9 PROGRESS REPORTS

The Senior Program Manager shall provide a monthly progress report to the Contracting Officer and COR via electronic mail. This monthly report shall contain but is not limited to the following:

6.9.1 Management Summary: Documenting by tasks any major problems/issues, current expenditures by work hours, and any significant progress or events;

6.9.2 Resource Expenditures: Funds expended during the reporting period, cumulative total, and funds remaining on the contract. Other information required include name, labor category, hours expended, cumulative hours expended on travel, and projected total hours for each individual working on this task;

6.9.3 Narrative: Description of work performed on task(s) during the reporting period and expected to be performed during the next month, including discussions of any problems/issues and recommendations for correction following due dates located in the delivery schedule. The Contractor shall report task status in accordance with the milestones and objectives identified in the appropriate project plan.

6.10 PROGRESS MEETINGS

The Senior Program 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 at the discretion of the Government at either the Government's facility, the Contractor's facility, or via teleconference.

6.11 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 PM - Program Manager

8.0 GOVERNMENT FURNISHED RESOURCES

The Government shall provide information, data and documents to the Contractor for work required under this task order. The Contractor shall use Government furnished information, data and documents only for the performance of work under this task order. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit written consent of the Contracting Officer. The Government will provide the contractor with access to any existing documentation that will assist in the performance of Task 2.1 – 2.4. This includes but not limited to, NRMC specific FEVS data, NRMC organizational charts, and employee information required to conduct focus groups.

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

- Laptops

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 Monthly Asset Management Report

The contractor shall 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 shall 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 4.0.

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, and FAR Clause 52.232-7, Payments under Time and Materials and Labor-Hours. 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/NRMC

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:

E-mail: [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]. 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 Flow down 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 task order, 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 access to CISA Sensitive Information, systems, networks, and reoccurring access to CISA facilities is not required under this SOW; therefore, contractor employees will not require DHS Fitness Determination to perform work.

Sensitive Information is defined in the DHS Instruction Handbook, 121-01-007, "The Department of Homeland Security, Personnel Security, Suitability and Fitness Program" as "Any information, the loss, misuse, disclosure, unauthorized access to, or modification of, which could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order

or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy. This definition includes one of the following categories of information:

A. Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. section 21 1-224; its implementing regulations, 6 C.F.R. Part 29; or the applicable PCII Procedures Manual; or

B. Sensitive Security Information (SSI), as described in 49 C.F.R. Part 1520; or

C. Sensitive but Unclassified Information (SBU) -For Official Use Only -, which consists of any other information which:

(1) If provided by the government to the contractor, is marked in such a way to place a reasonable person on notice of its sensitive nature;
(2) Is designated "sensitive" in accordance with subsequently adopted homeland security information handling requirements."

POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS

The procedures outlined below shall be followed for the CISA 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 CISA OCSO/PSD. Prospective contractor employees shall submit the below completed forms to their COR. 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 Positionsll
- 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 CISA OCSO/PSD. Specific instructions on submission of packages will be provided upon award of the contract.

CISA 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 CISA 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 CISA 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.

CISA OCSO/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the COR all CISA-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.