Department of Homeland Security (DHS)

STATEMENT OF WORK (SOW)

DHS/HQ
Office of the Chief Human Capital Officer (OCHCO)
Employee Experience

December 21, 2023

1.0 GENERAL

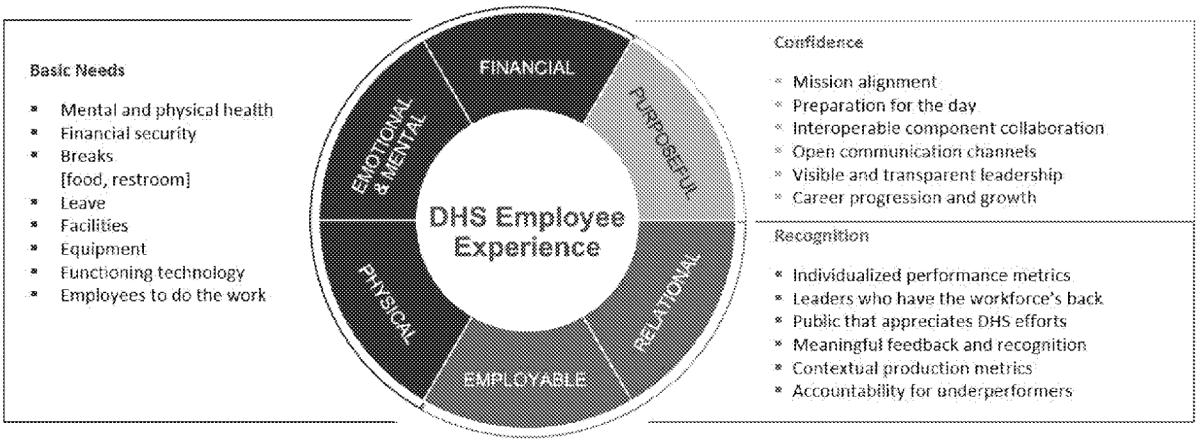
1.1 BACKGROUND

The Department of Homeland Security (DHS) has always been at the forefront of conducting programs to ensure we care and show concern for our employees, despite ongoing institutional challenges related to culture, morale, and employee engagement. The Department's ability to assess and shape its culture, which is steeped in the perceptions and experience of its 250,000 employees, will either limit or empower it to retain and recruit the workforce it needs to perform its mission.

At the leading edge of DHS' need to strengthen its ability to retain and recruit its workforce is its wide-scale effort to increase understanding of the "employee experience," and to ensure policies and programs directly address their needs and concerns. Without the ability to cull perceptions and input from employees in a way that empowers candor, ensures fidelity, and instills a sincere belief in employees that their feedback will be heard, DHS cannot be successful in shaping the culture needed to meet its workforce requirements. To date, various mechanisms have been established to gather, synthesize, analyze, and implement employee driven solutions, including focus groups, pulse surveys, key stakeholder interviews, and field tests. This effort is being led by the Strategic Talent, Empoloyee Engagement & Retention (STEER) (formerly known as Strategic Talent Recruitment, Inclusive Diversity, and Engagement (STRIDE)) division within DHS's Office of the Chief Human Capital Officer (OCHCO), in close coordination with stakeholders across all DHS Components.

The foregoing scope of work will facilitate the further development of these capabilities and to further institutionalize the new Employee Experience Framework ("Framework"). DHS cannot afford less than the strongest and most suitable vendor to help deliver on this broad-scale, complex, and timely work at such a pivotal time for the department; the risk of not having the appropriate talent and skills for mission delivery in the Department's workforce presents too great of a potential cost to the safety of the American public.

The Employee Experience Framework:



This procurement will provide staffing and expertise for a wide range of requirements related to empowering and acting on employee voice, in order to directly improve the daily work experiences of DHS employees.

1.2 SCOPE

DHS is a large, complex, geographically distributed agency with multiple and very distinct mission sets, cultures, and workforces. This work will reach across all elements of the Department and requires the capacity to manage projects, information, and data pertaining to an employee population of almost 250,000 individuals. It also requires political acumen, flexibility, and the capacity to adapt and shift in response to what is discovered while gathering employee voice. Close coordination with STRIDE/OCHCO is required. The contractor shall provide a dedicated team of personnel complete with the necessary level of experience and subject matter expertise required to perform all scope task areas as represented in the paragraphs below. This includes experience within the Federal Government on projects covering a very large (250,000+), highly distributed workforce with multiple complex missions that include frontline workforce and HQ workforce elements.

The scope of these requirements includes all staffing and support costs, as well as travel, supplies and equipment necessary to perform the full spectrum of services required

1.3 OBJECTIVE

The objective of this procurement is to support, refine, and expand the already in-process work related to the Framework. Ultimately, the goal is to support the Department's ability to attract, empower, and retain a high-performing workforce that can meet the needs of the mission. The requirements articulated within, if performed satisfactorily, will instill credibility in the Department, offer a source of action-focused collaboration support, and will increase effective coordination by Components and HQ Management Lines of Business.

1.4 APPLICABLE DOCUMENTS

The following documents are applicable the foregoing statement of work.

1.4.1 Compliance Documents
N/A

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

- DHS Employee Experience Framework
- President's Management Agenda Priority 1: Strengthening and Empowering the Federal Workforce

2.0 SPECIFIC REQUIREMENTS/TASKS

Support & Expertise
Work within the DHS environment is preferred. The contractor should demonstrate experience in testing and implementing an enterprise-wide approach to gauging and reporting on employee experience in a fast-paced and high-visibility environment requiring frequent and on-demand briefings to Cabinet-level leadership at the Secretary level of a very large agency. In addition to using existing data sources such as the annual Federal Employee Viewpoint Survey, pulse surveys, and relevant HR data for the work detailed below, the contractor shall demonstrate experience with conducting original/primary research throughout the cycle of surveys, focus groups, field tests, and pilot tests and reporting/making recommendations and implementing programs based on research, industry standards, observation and analysis. The contractor shall additionally demonstrate experience with creating processes and mechanisms for follow-up on action and adoption of recommendations, and in the development, deployment, and use of tools for issue-tracking.

Delivering DHS' employee experience organizational strategy requires strong facilitation and human-centered design skills to be able to both mold the experience as it unfolds and ensure the structure is robust enough to be effective. It also requires I/O Psychology experience, Coaching skills and large-scale change, culture expertise, excellent communications credentials and operational follow-through to be able to create lasting change. It will also require ability by the contractor to step-into the operational delivery of a strategy mid-stream; and an ability to quickly understand and manage a smooth transition period in which there is a short period of time to absorb programmatic knowledge, context, and the landscape of DHS policies and processes, and continue action in a manner that does not disrupt the existing schedule and cadence of activity. To that end it is desirable for the contract to have access to background cleared, certified, and skilled personnel who can quickly receive appropriate access to the DHS environments in place to provide these critical services with minimum transition and without delays.

2.1. TASK ONE - Employee Experience Focus Groups

- Contractor shall support up to four (4) Employee Experience focus group sprints per year with DHS Component organizations. Each sprint will include up to two organizations, two sites per organization, one full week of focus groups per site.
- Focus groups will follow existing protocols designed to align with the DHS Employee Experience Framework.
- Use data-driven methods to help identify DHS organizations for focus groups (FEVS scores, pulse surveys, etc.).
- Provide logistics related to focus groups, coordinating with sites on communications, scheduling, space, travel, virtual environments, and other relevant issues.
- Gather organizational background and context information in order to effectively prepare for focus groups – this may include online research, workforce data, FEVS and other data, conversations with key stakeholders, etc. – so that the team are informed and prepared.
- Provide consultation, technical assistance, and support for the onsite and virtual focus groups.
- Provide expert facilitation for the focus groups to be conducted at DHS locations around the United States and virtually, as part of a collaborative team that includes DHS and Component staff.
- Provide training to DHS/Component Staff teams to continue to develop in-house facilitation capabilities.
- Record and analyze the qualitative feedback from the sessions, leverage other qualitative and quantitative data as appropriate, and make recommendations for action.
- Design and deliver briefings and written reports to local, Component, and DHS Leadership on the results of the focus groups and analysis.
- See task 5 regarding conducting culture assessments, which is related but separate work and should be integrated with employee experience activities and initiatives.

2.2 TASK TWO - Surveys and Analysis

- Support DHS-Wide Pulse Survey Program – provide expert assistance in designing questions that are aligned with the Employee Experience Framework or other leadership concerns, analyzing results, and providing recommendations for action.
- Develop, administer, and analyze assessments for focus groups and field tests
- Create a survey to support culture assessments described in Task 5 below.
- Provide prompts for a DHS-managed ideation platform to solicit input from employees that ties to the new DHS Employee Engagement Framework or other leadership concerns.
- Develop and implement standardized Stay Interview questions for use across the enterprise.

2.3 TASK THREE - Employee Experience Field Tests

- Design and execute up to four (4) on-the-ground field tests/pilot projects/jump teams per year as part of a team that includes DHS and Component representatives. Field tests will be identified as outcomes of a variety of the already-described activities, including focus groups, and survey data analysis, or in working with

Component stakeholders. Field test execution will include design, logistics, planning, training participants in field test teams, as well as analysis and assessment.

- Design and deliver briefings and written reports to local, Component, and DHS Leadership.
- Develop recommendations and solutions for Component, DHS OCHCO and Management Directorate leadership based on field test results

2.4 TASK FOUR -Support for Committees and Working Groups

- Provide support in all capacities for multiple committees and working groups, including creating agendas, facilitating sessions, creating slide decks, taking notes, generating minutes, creating/maintaining governance documents, soliciting and organizing participation and supporting information sharing and exchange among membership.

2.5 TASK FIVE - Culture Assessments

- Contractor shall support all aspects of up to four (4) organizational culture assessments, to be identified by OCHCO, and delivered to DHS organizations as part of a collaborative team that includes DHS employees. Specifically, this includes actions to develop of questions for surveys, focus groups and interviews; designing appropriate survey and focus group populations; conducting interviews and focus groups; consolidating input and providing quantifiable themes from responses; performing analysis to identify root causes underlying symptomatic behaviors; developing recommendations for solution; and writing assessment reports, executive summaries, developing briefings, and generating related communications content to share findings. Climate assessments should be completed and delivered within a 12-month period.
- Review current culture assessment and consultation models and recommend enhancements in methodology, delivery, data synthesis, solutions development, and follow-through/actioning that strengthen return on investment. Recommend ways to identify and track specific, measurable outcomes for monitoring and reporting of progress.
- Coordinate logistics and provide related support for culture assessments, including: coordinating with customers on communications, scheduling meetings, focus groups and interviews; planning for and providing logistics support for culture assessment meetings (whether in scheduling and arranging for physical office space for in-person, or for virtual meetings in an online environment); ensuring accommodations and other technical needs are met for participation by interviewees and participants, and other relevant issues.
- Provide expert cultural facilitation for interviews and focus groups ranging from small (up to 5 participants) to mid-size (up to 15-20), ensuring coverage for a statistically sound sample size of the organization's population (organizations range in size and may include workforces as large as- approx. 2,000 employees), as part of a collaborative team that includes DHS employees.
- Record and analyze the qualitative feedback from the sessions, leverage other qualitative and quantitative data as appropriate (e.g., workforce demographic data,

applicant flow data, FEVS and other organizational culture data, etc.), and make recommendations for action. Recommendations for action may be informed by standard industry practices, academic studies, and other such researchable sources of information.

- Contractor will write and assemble an assessment report with recommendations for culture assessment customer's action/change, consolidating input from, and working as part of a collaborative team that includes DHS employees.
- Contractor will develop recommendations and protocols for culture assessment customer's follow-up actions to measure/gauge progress.

2.6 TASK SIX - General Program Support

- Provide general program support for to STRIDE/OCHCO for the execution of related projects and programs.
- Create reports, decision memos, slide decks/presentations, Internet/Intranet/SharePoint content and other supporting communications materials.
- Schedule and staff meetings and other events as required.
- Work across lines of effort to create alignment and efficiencies.
- Facilitate discussion/planning of overall Employee Experience Strategic Plan with appropriate stakeholders and parties.
- Develop an operations or roll-out plan to deliver tools and guidance to Components, including a way to measure and report on progress.

3.0 CONTRACTOR PERSONNEL

3.1 Qualified Personnel

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

3.2 Continuity of Support

The Contractor shall ensure that all contract support personnel are present for all hours of the workday (see section 4.4). If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., replacement personnel shall be provided, the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) prior to employee absence.

3.3 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* personnel 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.

All Key personnel is listed below:

- Program Manager

The required qualification for the program manager position is detailed below.

In addition to the Key Personnel, the contactor shall provide a work force possessing the skills, knowledge, clearances (where applicable), and training to satisfactorily perform the task order requirements stated herein. The contractor shall fill positions needed to support the work in this SOW with qualified personnel by the start date at a minimum.

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

Program Manager

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

The Program Manager will have at minimum a Bachelors degree and have the following education experience:

- Five (5) years of professional experience in project management and/or employee engagement related field with the most recent three (3) years of work experience related to employee engagement
- Must have experience providing operational oversight and leadership to manage technical, programmatic, and project goals and objectives are met and identify possible program risks
- Professional experience with implementation of programmatic solutions
- Preferred experience in federal government
- Preferred experience in and with familiarization with employee engagement and diversity, equity, inclusion and accessibility

The Program Manager shall be available to the COR via telephone between the hours of 9:00 A.M. and 5:00 P.M. EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 48 hours of notification.

3.4 Employee Identification

3.4.1 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.

3.4.2 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.

3.6 Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees 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 Program Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

3.7 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

N/A

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.

4.2 PERIOD OF PERFORMANCE

The period of performance for this contract is a one-year base period with two (2) one-year option periods as follows:

Base Period	April 4, 2024 – April 3, 2025
Option Year 1	April 4, 2025 – April 3, 2026
Option Year 2	April 4, 2026 – April 3, 2027

4.3 PLACE OF PERFORMANCE

Contractor personnel are expected to work remotely with occasional onsite meetings being conducted in various DHS locations throughout the Continental United States of America (CONUS). The Government shall notify the contractor of any change to location 15 days in advance. On-site or remote location shall be determined by the government.

4.4 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 9:00 am and 5:00 pm 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.

The Contractor is hereby advised that government personnel observe the following 11 federal holidays:
New Year's Day
Martin Luther King's Birthday
President's Day
Memorial Day
Juneteenth National Independence Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

In addition to the days designated as holidays the government may observe the following:

- Any other days(s) designated by Federal Statute
- Any other designated day(s) by Executive Order
- Any other designated day by President's Proclamation. This includes Inauguration Day (Washington D.C. Metropolitan area only). Observation of such day(s) by government personnel shall not be a reason for an additional period of performance, or an entitlement of compensation.

4.4.1 GOVERNMENT DISMISSAL AND CLOSURES

In cases of emergencies, severe weather conditions, natural disasters, and other incidents that cause disruptions of Government operations - operating status shall be in accordance with the Office of Personnel Management (OPM) Operating Status. Announcement on the status of Government operations in the Washington, D.C. area will be available at Current Status (opm.gov).

Contractors work schedule shall be in accordance with the requirements below:

1. If the Government is open, the Contractor is expected to report at their scheduled time.
2. If the Government is delayed opening, the Contractor is expected to report as instructed on the OPM website.
3. If the Government is closed, the Contractor is not expected to report to the office.
4. Contractor telework may be authorized at the Government's discretion. If services are determined to be needed during closure, the Contractor's PM shall provide a list of Contractors that will be teleworking and the work to be completed during the closure to the COR via e-mail NLT 9AM EST. Final approval shall be made by the COR.

4.5 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.

4.6 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 via teleconference.

4.7 PROJECT PLAN

The Contractor shall provide a final Project Plan at the Post Award Conference for Government review and comment. The COR will review and respond in accordance with Section 8.2 below.

4.8 BUSINESS CONTINUITY PLAN

4.8.1 The Contractor shall prepare and submit a final Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 30 business days after the date of award and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to

maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

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

4.8.2 Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 4 hours of activation or as directed by the Government, and shall be sustainable until the emergency is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life-threatening emergency, the COR shall immediately contact the Contractor Program Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occurs, the Contractor Program Manager and the COR shall promptly open an effective means of communication and verify:

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

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

4.9 PROGRESS REPORTS AND PROGRAM REPORTS

PROGRESS REPORT: The Program Manager shall provide a bi-weekly Progress Report to the COR, Government PM, and Division Chiefs via electronic mail. This report shall include a detail of all Contractor work performed by task number, including deliverables in progress, and completed. Report on technical progress, schedule status, and any Contractor concerns or recommendations for the previous reporting period.

PROGRAM REPORT: The Program Manager shall provide a monthly Program Report to the Contracting Officer, COR, and Government PM via electronic mail. This report shall include a

summary of all Contractor work performed by task number and CLIN, including a breakdown of labor hours by labor category, all direct costs by line item, contract burn rate, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

4.10 PROGRESS MEETINGS AND PROGRAM REVIEW MEETING

PROGRESS MEEING: The Program Manager shall meet with the COR Government PM, and Division Chiefs on a bi-weekly basis to present deliverables, discuss progress, schedule, exchange information and resolve emergent technical problems and issues. These meetings shall take place via teleconference or at a predetermined location by the COR and coordinated with the Contractor's PM.

PROGRAM REVIEW: The Program Manager shall meet with the Contracting Officer, COR, Government PM, and Division Chiefs monthly to present deliverables, review program cost, discuss progress, schedule, exchange information and resolve emergent technical problems and issues. These meetings shall take place via teleconference or at a predetermined location by the COR and coordinated with the Contractor's PM.

4.11 GENERAL REPORTING 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).

4.12 SECTION 508 COMPLIANCE

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

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

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

2018, or any successor publication.

5.0 GOVERNMENT TERMS & DEFINITIONS

5.1 COR – Contracting Officer's Representative
5.2 DHS – Department of Homeland Security
5.3 CO – Contracting Officer
5.4 STRIDE – Strategic Talent Recruitment, Inclusive Diversity, and Engagement
5.5 OCHCO – Office of the Chief Human Capital Officer

6.0 GOVERNMENT FURNISHED RESOURCES

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

- Laptop

The Government will provide all necessary information, data and documents to the Contractor for work performance. 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.

6.1 RECORDS MANAGEMENT OBLIGATIONS

The term Federal record:

1. includes DHS/STRIDE records.
2. does not include personal materials.
3. applies to records created, received, or maintained by Contractors pursuant to their DHS/STRIDE contract.
4. may include deliverables and documentation associated with deliverables.

6.1.1 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. chapters. 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.

6.1.2 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.

6.1.3 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.

6.1.4 STRIDE 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 STRIDE 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 STRIDE. The agency must report promptly to NARA in accordance with 36 CFR 1230.

6.1.5 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 Task Order. 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 DHS 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 Task Order. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph 6.1.4.

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

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

6.1.8 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.

6.1.9 All deliverables under the contract are the property of the U.S. Government for which STRIDE shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.

6.1.10 Training

All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take DHS-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.

6.2 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.

7.0 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 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.

8.1 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.

8.2 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.

8.3 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.

9.0 DELIVERABLES

The Contractor shall consider items in **BOLD** as having mandatory due dates.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	4.6	**Post Award Conference**	5 business days after date of award	COR, CO, STRIDE Leadership Team
2	4.7	**Final Contractor Project Plan**	4 business days after the post award conference	COR, Contracting Officer
3	4.8	**Original Business Continuity Plan**	30 days after date of contract award	COR, Contracting Officer
4	4.8	**Updated Business Continuity Plan**	Annually, on the 30th day of each exercised option	COR, Contracting Officer
5	4.9	**Progress Reports**	Monthly, on the 5th of every month	COR, Contracting Officer
6	2.2	Survey to Support Culture Assessments	To be established based on the project plan	STRIDE Leadership Team
7	2.2	Stay Interview Questions	To be established based on the project plan	STRIDE Leadership Team
8	2.5	Recommendations to enhance current culture assessment	To be established based on the project plan	STRIDE Leadership Team

10.0 CLAUSES

FAR 52.224-3 Privacy Training – Alternate I (DEVIATION 17-03) (July 2023)

(a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with

other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).
(b) The Contractor shall ensure that initial privacy training, and annual privacy training, thereafter, is completed by contractor employees who—
(1) Have access to a system of records;
(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).
(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.
(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.
(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.
(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—
(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or
(3) Design, develop, maintain, or operate a system of records.

(End of clause)

INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

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

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive

information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually, and the COR will provide notification when a review is required.

(End of clause)

HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information.

As prescribed in (HSAR) 48 CFR 3004.470-4(b), insert the following clause:

SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)

(a) *Definitions*. As used in this clause—
Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples

of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);

(B) Date of birth (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

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

(b) *Handling of Controlled Unclassified Information.*

(1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.
(3) The Contractor shall not maintain SPII in its invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions. It is acceptable to maintain in these systems the names, titles, and contact information for the Contracting Officer's Representative (COR) or other government personnel associated with the administration of the contract, as needed.
(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) *Incident Reporting Requirements.*

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.
(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.
(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a *FIPS 140-2/140-3 Security Requirements for Cryptographic Modules* validated cryptographic module identified on https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.
(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.
(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, *Incident Response*, to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems*, Contractors shall also provide as many of the following data elements that are available at the time the incident is

reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime Contractor location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);
(v) Contracting Officer POC (address, telephone, and email);
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

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

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

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

(i) Inspections;
(ii) Investigations;
(iii) Forensic reviews;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate (ATO), if applicable.

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

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

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

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

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

(End of clause)

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

(h) *Authority to Operate.* The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems* (Version 13.3, February 13, 2023), or any successor publication; and the *Security Authorization Process Guide*, including

templates. These policies and templates are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(i) *Security Authorization Package*. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) *Independent Assessment*. Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800–53, *Security and Privacy Controls for Information Systems and Organizations*, or successor publication, accessible at *https://csrc.nist.gov/publications/sp*. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or
(ii) Submitting the updated SA package directly to the COR.

(3) *Security Review.* The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the

Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), 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 government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Federal Reporting and Continuous Monitoring Requirements.* Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2015 DHS Information Security Performance Plan, or successor publication, accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

3052.204-73 NOTIFICATION AND CREDIT MONITORING REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION INCIDENTS (JULY 2023)

(a) *Definitions.* Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive
and may alone present an increased risk of harm to the individual.

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits);
(ii) Date of birth (month, day, and year);
(iii) Citizenship or immigration status;
(iv) Ethnic or religious affiliation;
(v) Sexual orientation;
(vi) Criminal history;
(vii) Medical information; and
(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) *PII and SPII Notification Requirements.*

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;
(ii) A description of the types of PII or SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(c) *Credit Monitoring Requirements.* The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.
(3) Establish a dedicated call center. Call center services shall include:
(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

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

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

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS OCSO-HQS PSD. Prospective contractor employees shall complete and submit a combination of the below forms to the DHS OCSO-HQS PSD. The Standard Form (SF) 85 must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85 signature pages and other completed forms must be given to the OCSO-HQS PSD no less than thirty days before the start date of the contract or thirty (30) days prior to the requested entry on duty date, for all contractor employees whether a replacement, addition, subcontractor employee, or vendor. OCSO-HQS PSD does not process any requests until the contract has been awarded and released from PRISM to FPDS and ERA by extension.

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

Only complete packages will be accepted by the DHS OCSO-HQS PSD. Specific instructions on submission of packages will be provided upon award of the contract.
The DHS OCSO-HQS PSD may, as it deems appropriate, authorize, and grant a favorable Entry on Duty (EOD) decision based on preliminary checks. A favorable EOD decision allows a contractor employee to commence work temporarily prior to the completion of the full background investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable fitness determination will follow. In addition, a favorable EOD or fitness determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD or fitness determination by the DHS OCSO-HQS PSD. Limited access to Government buildings is allowable without an EOD decision if the Contractor is escorted by a Government employee and the purpose of the visit is to attend a limited number (less than 5) of required briefings or nonrecurring meetings in order to facilitate the transition of a contract. The intent of this statement is to allow a minimum amount of meetings/transition attendances to prepare for a new contract.

The DHS Security Office shall be notified of all terminations /resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative

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

When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Depa1iment security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

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

- Your POC at the Security Office is:

  DHS OCSO/PSD Security Customer Service Center
  Telephone: [redacted]
  E-mailbox: [redacted]