DEPARTMENT OF HOMELAND SECURITY (DHS)
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)
EMERGENCY COMMUNICATIONS DIVISION (ECD)

STATEMENT OF WORK (SOW)
FOR
ECD PROGRAM EFFICIENCIES

1.0 GENERAL

This effort will support the Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Division (ECD) Front Office (FO) by conducting a full check to empower CISA's dynamic workforce and improve organizational effectiveness and efficiencies.

1.1 BACKGROUND

CISA is the Nation's risk advisor, and as such is responsible for enhancing the resilience and security of the Nation's critical infrastructure. This responsibility is a partnership with more than 32 million officials working across all vital nationwide services that support the Nation's critical infrastructure, public safety, and national security and emergency preparedness communities. The partnership and effective execution of the CISA mission requires strategic teambuilding and the effective coordination and collaboration of a broad spectrum of federal, state, local, tribal and territorial governments, private sector, international partners, and non-governmental organizations. It requires continual (24 hours a day and 7 days a week) cyber and physical security situational awareness to include analysis, incident support, cyber-response/ analysis and defensive capabilities, and interoperable emergency communications capabilities supporting critical non-governmental organizations, the Federal, State, Local, Tribal and Territorial governments; the private sector and international partners.

CISA provides priority service capabilities to approximately 10 million officials within in the vital nationwide services community. Within this group of officials are approximately 300,000 experts supporting emergency communications. The community of 300,000 emergency communications officials are found supporting all 55 of the national critical functions. CISA collaborates with partners across the spectrum of public safety, critical infrastructure, and national security and emergency preparedness to enhance the ability of these vital nationwide services to continue sharing information using emergency communications in day-to-day mission essential activities as well as during heightened incidents.

CISA ECD supports nationwide partnerships and delivery of technical assistance support, and provision of priority voice, video, data and information services capability to enhance interoperable communications for these vital nationwide service officials. The ECD is currently in an expanding, startup mode needing to scale support services from a current base of customers receiving priority service capabilities totaling just under a half million customers to reach the targeted 10 million

customers of priority previously mentioned. At the same time, ECD is expanding its partner base from current levels of 20,000 across the nation, to grow and include all 300,000 partners mentioned above, as the organization scales its services to meet this program target by the year 2033.

Emergency Communications face an increasing tempo of change in the evolution of technology and potential threats to cybersecurity. Commercial network services are advancing from fourth generation long term evolution to fifth generations telecommunications capabilities. Fiberoptic and cable technologies are advancing to tenth generation internet protocol delivery speeds with massive bits per second capabilities. Rapid advances in mobile edge computing and the need for zero trust security environments and supply chains, make the depth of knowledge needed a challenge in order to unify the broad scope of subject matter expertise in the information and communications technology community.

2.0 PURPOSE

The purpose of this requirement is to enhance the federal staff operating paradigm to an agile, adaptive, and fast-paced performance paradigm that will inspire government, private sector, and non-government partners to increased collaboration in order to achieve the CISA mission and reduce nationwide systemic risk.

3.0 SCOPE

The contractor shall provide all expertise, materials, personnel, and services required to perform tasks as identified in this SOW. The scope of this SOW includes the following tasks related to organizational analysis to support the implementation of CISA ECD's long-range improvement efforts and related activities:

A. Organizational benchmarking, baselining and rebaselining (Phase 1)
B. Individualized employee engagement strategies and needs based assessments (Phase1)
C. Process improvement, obstacle mitigation, and phased implementation plan (Phase 2)
D. Training Support (Phase 2)
E. Workspace Optimization (Phase 3)
F. Remote work structure (i.e., policies, flexibility, impact, and options) (Phase 3)

4.0 SPECIFIC TASKS/REQUIREMENTS

4.1 Task 1: Organizational Benchmarking and Baseline(s)

The Contractor shall conduct an internal organizational benchmark and baseline(s) to confirm engagement and commitment to the CISA ECD mission. The Contractor shall provide a team of personnel with the proper skills and recent experiences with conducting organizational analysis and developing the products and deliverables required for this task order. Benchmarking is an important first step to achieve continuous improvement: it provides a structured approach to improve the performance of an organization by identifying and applying best practices and serves as a baseline to diagnose the drivers that impact performance. Baselining involves documenting the processes along with supporting documents (i.e., organizational roles, workflow, timing, metrics, etc.) to

determine the effectiveness of change and measure progress towards meeting intended goals.

The following support tasks are included as examples only. Actual tasks may include the following:

1. Developing and maintaining a plan for accomplishing internal benchmarking and baselining including strategy, objectives, methodology, activities, schedule, and milestones.
2. Facilitating group briefings and discussions in support of focused decision-making and providing draft and final reports relating to facilitated issues, action items, meeting minutes schedule and milestone updates and documentation. Sessions may occur weekly, monthly, or quarterly as determined by the Contracting Officer Representative (COR)/Alternative Contracting Officer Representatives (ACORs).
3. Developing and providing implementation strategies to conduct recurring baselining efforts to measure effectiveness and efficiency (i.e., monthly, quarterly, annually).
4. Preparing monthly progress reports and accomplishments to track progress (i.e., ECD quarterly contract review accomplishments).
5. Conduct quarterly comprehension and readiness checks to revive employee commitment to the process and cultivate a unified approach to organizational baselining.

4.2 Individualized Employee Engagement Strategies and Needs Based Assessments

The Contractor shall develop strategies to solicit employee feedback, encourage positive organizational citizenship, increase productivity, and support personal development goals. This effort requires identification of factors that are important to each employee and development of effective intervention strategies to bridge the gap between the employees current and desired state.

The following support tasks are included as examples only. Actual tasks may include the following:

1. Identifying staff, roles, core functions, interests, and challenges.
2. Developing strategies to uphold organizational core values, identify career paths and provide opportunities for growth.
3. Providing feedback to leadership to communicate sub-division specific trends, analysis and recommendations.
4. Developing strategies to align, people work, and competencies with CISA ECD's mission and vision.
5. Designing briefings to analyze interview, survey, and questionnaire results.

4.3 Task 3: Process Improvement, Obstacle Mitigation, and Phased Implementation Plan

The Contractor shall design an optimal organizational rhythm that aligns with the CISA's vision, giving the federal staff space to innovate and think deeply, resulting in increased performance that is more fluid, adaptable, and capable of executing in the startup environment.

The following support tasks are included as examples only. Actual tasks may include, but are not limited to, the following:

1. Interviewing, surveying, and questioning approximately 139 ECD employees to solicit their feedback and recommendations regarding all organizational improvement efforts and related activities.
2. Developing strategies to map, analyze, and redesign processes.
3. Gather and document lessons learned from organizational improvement efforts and related activities.
4. Developing strategies to improve cross-collaboration between sub-divisions and leverage organizational expertise.
5. Creating a phased implementation and succession plan that will evolve alongside the agency as it transitions from the current start-up posture to a unified mature posture.

4.4 Task 4: Training Support

The Contractor shall provide comprehensive support to develop a streamlined approach to reaching workforce training and development goals resulting from individual needs-based assessments.

Tasks may include, but are not limited to the following:

1. Identifying training gaps and mapping out individual plans and schedules to meet organizational and individual needs.
2. Conducting full scale virtual training seminars or workshops to assist employees with work/life balance, effective time management, conflict resolution, and diversity and inclusion.
3. Developing post training evaluations to obtain employee feedback.
4. Ensuring that training plans are consistent with the goals and objectives of organizational improvement efforts and related activities.
5. Maintaining a record of all employees that complete Contractor-led training engagements.

4.5 Task 5: Workspace Optimization

The contractor shall leverage existing departmental resources, best practices, and lessons learned to identify existing workspace optimization strategies; solicit employee feedback regarding their workspace (current and future); and analyze impacts to productivity and morale.

Tasks may include, but are not limited to the following:

1. Developing metrics to track employee perspectives as the organization transitions from the old-assigned seating model to an agile work environment.
2. Identifying activity-based workspaces designed to support the type of work that an employee needs to do (i.e., open areas for group work sessions, small conference rooms for

team meetings, video conference rooms for meeting with regional staff, isolated quiet areas, and spaces to make call without disrupting other colleagues).
3. Developing communications material to support change management efforts and employee awareness (i.e., shared workspace etiquette, fostering social cohesion and trust, and ensuring behavioral & cultural fit).
4. Providing recommendations to collect, analyze, and mitigate employee concerns.
5. Updating strategies as necessary to incorporate lessons learned.

4.6 Task 6: Remote Work Structure

The Contractor shall develop a series of assessments to solicit employee feedback regarding pre and post pandemic workplace trends, common challenges of remote work, lack of face-to-face supervision and interaction, lack of access to information, social isolation, and distractions at home, etc.

The following support tasks are included as examples only. Actual tasks may include the following:

1. Analyzing and consolidating results to communicate findings to target audiences.
2. Identifying resources to assist employees with navigating through their remote work environment.
3. Sharing success stories and other useful information to support long-term remote, hybrid, and traditional work schedules based on employee feedback.
4. Identifying the financial impact of long-term remote work structures (i.e., purchase of office supplies, equipment, home modifications, and other work-related expenses).
5. Developing a plan to establish a remote work culture that is based on employee feedback.

4.7 Task 7: Surge Support (Optional)

During the base and option year task order periods, the Contractor may be tasked ad-hoc to provide personnel within appropriate labor categories, and at the appropriate level of effort, for short durations in support of the programs as stated in this Scope of Work.

During the base and option year task order periods, there may be instances in which the Contractor will be required to provide surge support. This may increase the staffing level of the task order. In those instances, the CO will exercise the corresponding Contract Line Item Number (CLIN) or surge support and authorize the Contractor to perform for a not-to-exceed (NTE) number of hours based on the Contractor's proposed fixed labor rates. The Contractor shall perform all surge support in accordance with the Statement of Work tasks (1-6). The CO is the only individual able to authorize surge support. The Offeror must provide a plan to demonstrate management of requests for surge support and how these requests will be met. The Contractor shall be flexible to mission needs and able to provide surge support as requested by the CO. The Contractor shall provide additional ad hoc support in accordance with the statement of work as required.

Surge support may increase the staffing level of the task order. The Contractor should provide its

own blend of personnel with skill sets and qualifications that are consistent with their proposed approach to meeting the requirements of the solicitation.

4.8 Task 8: Transition (Optional)

The Contractor shall develop, document, and monitor the execution of a transition plan that may be used to transition tasks and materials to a new Contractor, or to the Government. The plan will incorporate an inventory of all services and materials developed that will be required to fully perform the services provided under this contract. The plan will include a schedule of briefings, including dates and time and resources allotted, that will be required to fully transition all materials developed to the follow-on Contractor, and will provide the names of individuals that will be responsible for fully briefing their follow-on counterparts. The plan is to ensure that the follow-on Contractor, or the Government, will be provided sufficient information and be fully briefed prior to the current expiration date of the contract, to provide adequate time for the new Contractor to have their personnel completely familiar with the requirements and in place on the turnover date. The Contractor shall plan for a thirty (30) business days transition period. The plan shall provide the contact information for contractor individuals who will be assigned to the transition team and identify their roles in the transition.

The Contractor shall participate in transition meetings with the program manager and project staff, and representatives of the successor Contractor. The purpose of these meetings is to review project materials and take preparatory steps to ensure an effective transition in Contractor support. The transition plan is due to the Government sixty (60) business days prior to the expiration date of the contract.

5.0 GOVERNMENT FURNISHED RESOURCES (GFR)

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

- Laptop and charging adapter (Laptop B Only)
- DHS E-mail Account
- DHS PIV Badge
- DataWatch Card (if applicable)
- Mobile Phone (DHS Program Manager and Contracting Officer approval required)

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

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

5.1 Property Inventory

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

Contractor will confirm receipt of CISA property purchased under this SOW with the assigned CISA Accountable Property Officer (APO) and COR within 5 business days of receipt.

[redacted]

5.2 Monthly Asset Management Report

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

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

5.3 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 5.0.

6.0 CONTRACTOR PERSONNEL

6.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW. Visiting contractor employees shall comply with all Government escort rules and requirements.

6.2 Key Personnel

The position specified below shall be considered essential to the work being performed under this task order. Before replacing any individual designated as *Key* by the Government, the Contractor

shall notify the CO, COR, and ACORs no less than fifteen (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 CO and COR. The Contractor shall not replace *Key* Contractor personnel without approval from the CO, COR, and ACOR. Contractor *Key* personnel shall not be assigned by the Contractor to more than one key position for this requirement.

The following Contractor positions are designated as Key for this requirement:

Project Manager *(100% Level of Effort estimated)*

The proposed Project Manager (PM) will provide the oversight and management required to perform the tasks described in Section 4.0 "Specific Tasks/Requirements" (including all subsections) of this SOW, as well as supervise and lead the Contractor team. The PM shall be a single point of contact for the CO, COR, and ACORs. It is anticipated that the PM shall be one of the senior level employees provided by the Contractor for this work effort. The proposed PM shall be a certified project management professional (or equivalent) with over eight (8) to ten (10) years of professional experience in project and task management, strategic planning, and meeting design and facilitation experience. Experience with emergency communications, familiarity with ECD, and an understanding of emergency communications and technology policy are highly recommended for this position. The PM shall be available to the COR in- person or via telephone between the hours of 8:00 a.m. and 5:00 p.m. Eastern Time (ET), Monday through Friday, less federal holidays, and shall respond to a request for discussion or resolution of technical problems within four (4) hours of notification.

During any absence of the PM, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this task order. The PM and all designated alternates shall be able to read, write, speak, and understand English. Additionally, the Contractor shall not replace the PM without prior approval from the CO, COR or ACORs.

6.3 CONTINUITY OF SUPPORT

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

6.4 EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level, and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and

requirements. All Contractor employees shall identify themselves as Contractors when their status is always not readily apparent and display all identification and visitor badges in plain view above the waist.

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

6.5 EMPLOYEE CONDUCT

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

6.6 REMOVING EMPLOYEES FOR MISCONDUCT OR SECURITY REASONS

The Government may, at its sole discretion (via the CO), 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 task order. The CO will provide the Contractor with a written explanation to support any request to remove an employee.

6.7 TERMINATIONS/RESIGNATIONS

The contractor will notify the Office of the Chief Security Officer (OCSO), COR, and ACOR of all terminations/resignations of contractor personnel assigned to this contract ten (10) working days before the last day of employment. In the event this notification is not possible, the OCSO and COR should be notified immediately. The contractor shall return to the OCSO 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 OCSO, COR, and ACOR 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.

7.0 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the CO and the COR no later than ten (10) business days after the date of award. The purpose of the Post Award Conference, which will

be chaired by the CO, 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 4200 Wilson Blvd., Arlington, VA 22203 or via teleconference.

7.1 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/ACORs not later than ten (10) business days after the Post Award Conference.

8.0 DELIVERABLES

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

a) All deliverables, if the delivery date falls on a Saturday or Holiday, which is on a day other than a Monday, the deliverable will be considered to have been received by the Government on the preceding workday. If the delivery date falls on a Sunday or a Monday holiday, the deliverable will be received on the following workday.

b) The contractor shall submit each deliverable as one file unless file size or other conditions warrant establishing multiple files and submit the table of contents in the same file as the main body of the deliverable. All deliverables must have a document control number and revision number.

c) In the event the contractor anticipates difficulty in complying with any delivery schedule, the contractor shall immediately notify the CO in writing, giving pertinent details, including the date by which it expects to make delivery; provided, however, that this data shall be informational only in character and that receipt thereof shall not be construed as a waiver by the Government of any contract delivery schedule, or any rights or remedies provided by law or under this contract.

d) The Government will have 10 business days to review and comment on deliverables. If the deliverable does not meet the noted criteria, the Government will return it to the Contractor for revision. Deliverables will be deemed "accepted" unless a rejection notice, in writing, from the CO is received within 10 business days after submission or the specified review timeframe as described in the task description.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	7.0	**Post Award Conference**	Not Later than ten business days after Date of Award (DOA)	N/A
2	7.1	*Draft Contractor Project Plan*	Not Later than ten business days after Date of Award (DOA)	COR, ACORs, Contracting Officer
3	7.1	**Final Contractor Project Plan**	Not Later than ten business days after the Post Award Conference	COR, ACORs, Contracting Officer
4	15.0	**Original Business Continuity Plan**	Not Later than thirty business days after Date of Award (DOA)	COR, ACORs, Contracting Officer
5	15.0	**Updated Business Continuity Plan**	Not Later than one year after Original Business Continuity Plan	COR, ACORs Contracting Officer
6	10.2	**Progress Reports**	10th business day of the month	COR, ACORs Contracting Officer
7	4.0	Program Briefing Materials	Draft due at least five (5) business days before briefing	COR, ACORs
8	4.0	Program Analysis Report	Ongoing effort	COR, ACORs
9	4.0	Fact Sheets and One Pagers	Draft due 5-10 business days after initial assignment	COR/ACORs
10	4.0	Strategic messaging support tools (e.g., talking points, emails, presentations, graphics)	Draft due 5-10 business days after initial assignment	COR/ACORs
11	4.0	SIP email inquiry responses	Draft due one business day after receipt	COR/ACORs
12	4.0	Performance Management and Strategic Planning program support products (e.g., white papers, surveys, questionnaires, roadmaps, strategies, tracking devices, etc.)	Draft due 5-10 business days after receipt	COR/ACORs
13	4.0	Meeting Agenda	Two business days before meeting	COR/ACORs
14	4.0	Minutes from Meetings	Two business days after meeting	COR/ACORs

15	4.0	Responses to ad hoc requests for information or analysis from internal or external stakeholders	Draft is due two business days after receipt	COR/ACORs
16	4.0	Program management assistance tools, templates, and handbook	10-30 business days after initial assignment	COR/ACORs
17	4.0	Support ECD federal program staff	Initial response within one business day of inquiry	COR/ACORs
18	4.0	Meeting Planning, including site research and determination of requirements, development of meeting materials, on-site support services, and after-action documentation.	30-60 calendar days after assigned	COR/ACORs

9.0 INSPECTION AND ACCEPTANCE

Program manager and/or technical leads will review draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance within the guidelines/requirements of the contract and will inform the Contractor of its acceptability. The Contractor shall ensure the accuracy and completeness of all deliverables in accordance with referenced policy, regulations, laws, and directives. Reports and presentations shall be concise and clearly written. Errors, misleading or unclear statements, incomplete or irrelevant information, and/or excessive rhetoric, repetition, and "padding", or excessive length if a page limit is imposed, shall be considered deficiencies and will be subject to correction by the Contractor at no additional cost to the Government. Unless otherwise indicated, the Government will require 10 workdays to review and comment on deliverables. If the deliverable does not meet the noted criteria, the Government will reject it.

A rejected deliverable will be handled in the following manner:

- After notification that the deliverable did not meet the acceptance criteria the Contractor shall resubmit updated/corrected version ten (10) workdays after receipt of Government comments.
- Upon the Contractor's re-submission, the Government will reapply the same acceptance criteria.

10.0 STANDARD DELIVERABLE DISTRIBUTION AND REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (e.g., Windows Operating System [OS] and Microsoft Office Suites).

All work products shall meet professional standards to include no spelling and grammatical errors and adhere to the requirements outlined in the SOW. In addition, all work products must comply with DHS and CISA branding guidelines. It is the Contractor's responsibility to understand branding requirements and ensure all work products are compliant. Any work product containing spelling, grammatical, and/or branding issues shall be considered incomplete thus not qualified for government acceptance.

10.1 PACKAGING AND MARKING

All information submitted to the Government, whether submitted electronically, through the postal system, or in person, shall clearly indicate the Project Title, Contract Number, and the names of the CO, Contract Specialist (CS), COR, and ACORs.

All postage and fees related to submitting information including forms, reports, submittals, etc. to the CO, CS, or the COR/ACOR shall be paid by the Contractor.

Contractor will use best practices for packaging.

10.2 PROGRESS REPORTS AND MEETINGS

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

The PM shall be available to meet with the COR/ACORs upon request to present deliverables, discuss progress, exchange information, and resolve emergent technical problems and issues. These meetings shall take place at the Government's facility.

11.0 OTHER APPLICABLE CONDITIONS

11.1 Security

This Task Order requires all Contractors to be U.S. citizens and obtain DHS suitability.

POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR

CONTRACTS/ORDERS

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

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

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

Standard Form (SF) 85-P, —Questionnaire for Public Trust Positions‖
SF-85P Certification
SF-85P Authorization for Release of Information
FD Form 258, —Fingerprint Card (2 copies)
DHS Form 11000-6 —Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement
DHS Form 11000-9, —Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act

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

The DHS OCSO/PSD may, as it deems appropriate, authorize and grant a favorable Entry on Duty (EOD) decision based on preliminary checks. A favorable EOD decision allows a contractor employee to commence work temporarily prior to the completion of the full background investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable Fitness determination will follow. In addition, a favorable EOD or Fitness determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD or Fitness determination by the DHS OCSO/PSD.

Limited access to Government buildings is allowable without an EOD decision if the Contractor is escorted by a Government employee and the purpose of the visit is to attend a limited number of

required briefings or nonrecurring meetings in order to facilitate the transition of a contract The intent of this statement is to allow a minimum amount of meeting / transition attendances to prepare for the new contract.

The DHS OCSO/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer's Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

11.2 Period of Performance

The period of performance for this effort is one (1) eight-month base period, and two (2) twelve-month option periods.

- Base Period: 8/1/2024 through 4/30/2025
- Option Period 1: 5/1/2025 through 4/30/2026
- Option Period 2: 5/1/2026 through 4/30/2027

11.3 Place of Performance

Work performed under this task order will be performed at either the Government or Contractor facilities, with allowances for frequent local travel between the Contractor and Government facilities in the Washington, DC metropolitan area. The ECD facility is currently located at 4200 Wilson Blvd. in Arlington, Virginia 22203.

11.3.1 Contractor Telecommuting Remote Personal Residence Work Locations

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

11.3.2 Contractor Labor Rates Charged While Telecommuting

The contractor shall charge the same applicable fixed hourly rate as for a Contractor site for those

contractor personnel when they telecommute at their designated telecommuting location.

12.0 HOURS OF OPERATION

Contractor support shall generally be performed between the hours of 8:00 a.m. and 5:00 p.m. Eastern Standard Time (EST), Monday through Friday (except on the following 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.

• New Year's Day	January 1st
• Birthday of Martin Luther King Jr.	Third Monday in January
• Inauguration Day	January 20th for each fourth year
• President's Day	Third Monday in February
• Memorial Day	Last Monday in May
• Juneteenth National Independence Day	June 19th
• Independence Day	July 4th
• Labor Day	First Monday in September
• Columbus Day	Second Monday in October
• Veterans Day	November 11th
• Thanksgiving Day	Fourth Thursday in November
• Christmas Day	December 25th

Government closure may occur due to Presidential Executive Order and other unforeseen circumstances (i.e., Christmas Eve – December 24th, inclement weather, etc.).

13.0 TRAVEL

The Contractor shall maximize the use of video conferencing and virtual meeting platforms in lieu of travel. Contractor travel may be required to support this requirement, including but not limited to participation in meetings, conference activities, program reviews, and site visits. 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 (if allowed). The Contractor shall request authorization from the COR/ACORs at least two weeks prior to the commencement of Contractor travel. The Government will not reimburse local travel (i.e., within a fifty [50] mile radius of the assigned worksite).

14.0 OTHER DIRECT COSTS (ODCs)

All material required for performance under this task order that are not Government-furnished, are to be acquired by the Contractor as authorized by the COR, including regional meeting venues and stakeholder participation travel support. Ownership of non-consumable supplies acquired by the Contractor with Government funds, for performance of this task order, shall vest with the Government. The Contractor shall include a detailed description of all proposed ODCs to the COR for this task order.

ODC examples include:

- Licensing for various tools to create engaging and informational videos.
- Workshop and team exercise materials
- Assessments
- Human Resources Tools and Resources
- Instructional Systems Design Tools and Resources

15.0 BUSINESS CONTINUITY PLAN

Contractor shall prepare and submit a 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 how the Contractor will account for their employees during an emergency
- A description of the Contractor's emergency management procedures and policy
- 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

15.1 Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within two hours of activation or as directed by the Government, and shall be sustainable until the emergency situation 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 make contact with the Contractor Project 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 occur, the Contractor Project Manager and the COR shall promptly open an effective means of communication and verify:

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

16.0 PROTECTION OF INFORMATION

Contractor access to information protected under the Privacy Act is required under this PWS.

Contractor employees shall safeguard all information obtained under this order (see applicable Security level in Section 7.1 above) against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

17.0 SECTION 508 REQUIREMENTS

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

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

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

17.1 Section 508 Requirements for Technology Services

a) When providing installation, configuration or integration services for ICT, the Contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

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

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

d) When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The Contractor

shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at https://www.dhs.gov/trusted-tester.

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

f) When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester.

g) When developing or modifying hardware components of ICT, including closed systems (for example – kiosks), the Contractor shall demonstrate conformance to the applicable Section 508 standards (including the Chapter 4 hardware requirements). Where the requirements in Chapters 4 do not address one or more functions of ICT, the Contractor shall demonstrate conformance to the Functional Performance Criteria specified in Chapter 3. The Contractor shall use a test process capable of validating conformance to all applicable Section 508 standards for hardware functionality delivered pursuant to this contract.

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

17.2 Section 508 Deliverables

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

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

c) Section 508 Accessibility Conformance Reports: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

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

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

18.0 RECORDS MANAGEMENT OBLIGATIONS

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. includes DHS/CISA records.

2. does not include personal materials.

3. applies to records created, received, or maintained by Contractors pursuant to their DHS/CISA contract.

4. may include deliverables and documentation associated with deliverables.

18.1 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.

18.2 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. 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.

18.3 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 [Agency] 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.

18.4 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 [Agency] 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).

18.5 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 [Agency] guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

18.6 The Contractor shall only use Government IT equipment for purposes specifically tied to

or authorized by the contract and in accordance with [Agency] policy.

18.7 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.

18.8 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.

18.9 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 [Agency] 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.

18.10 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.

18.11 Flow-down of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this section, 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.

19.0 DEFINITIONS

- Accountable Personal Property - An asset that meets one or more of the following criteria: (1) expected useful life is two years or longer and an asset value and/or acquisition cost of $5,000 or more; (2) that is classified as sensitive; (3) for which accountability or property control records are maintained; (4) Capitalized personal property, (5) Leased property that meets accountability standards, or (6) otherwise warrants tracking in the property system of record. Current accountable personal property information may be obtained through the ECD APO Office at [redacted]
- Capitalized Personal Property - Non-expendable personal property with an acquisition cost over an established threshold and a normal life expectancy of two years or more. Current Capitalization Threshold information may be obtained through the ECD APO Office at [redacted]
- Contract Property - Contract property refers to both Contractor-Acquired Property

(CAP) and GFP, in the possession of contractors.

- Contractor Acquired Property (CAP) - Property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title.
- Government Furnished Property (GFP) - Property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. NOTE: GFP may also be referred to as Government Furnished Equipment (GFE), the two terms are interchangeable.
- Leased Property - Property that is not owned by DHS, but that is leased by the Government under terms as stipulated in the lease agreement (this excludes the leasing of property by contractors in the performance of a contract).
- Sensitive Personal Property - All items, regardless of value, that require special control and accountability due to unusual rates of loss, theft, or misuse; national security or export control considerations. Such property includes but is not limited to, weapons, ammunition, explosives, information technology equipment with memory capability, cameras, and communications equipment. Current sensitive personal property information may be obtained through the ECD APO Office at [redacted]

20.0 PROPERTY ACCOUNTABILITY

- When contractors are furnished with GFP, DHS barcodes will not be removed. In all GFP cases, the Government retains title to the property.
- It is the contractor's responsibility to use contract property as it was authorized, and for the purpose intended. In the event the contractor uses contract property for other purposes without written authorization from the CO, the contractor may be liable for rental, without credit, of such items for each month or part of a month in which such unauthorized use occurs.
- Contractor is directly responsible and accountable for all contract property in its possession in accordance with the requirements of the particular contract; this also includes any contract property in the possession or control of a subcontractor.

20.1 Physical inventory:

In addition to requirements provided under the contract's government property clause,

- The Contractor shall, minimum annually, perform, record, and disclose physical inventory results of CAP and GFP to the ECD APO Office at cs&cassetmanagementteam@hq.dhs.gov, PA and/or COR/ACORs
- Annual inventory results will be completed, certified and submitted by close of

business 31 May each year or as directed to the ECD APO Office at [redacted] PA and/or COR/ACORs

- The Contractor shall, upon request, perform, record, and disclose physical inventory results of CAP and GFP to the ECD APO Office [redacted], PA and/or COR/ACORs
- As requested inventory results will be completed, certified and submitted, in the timeframe defined at the time of request, to the ECD APO Office at [redacted], PA and/or COR/ACORs

20.2 Property Disposal

- All documentation and goods are the property of the United States Government and, if applicable, the contractor shall return or destroy appropriately upon request. The contractor shall comply with applicable government rules and regulations for disposal of government property. Further, the contractor shall provide necessary information to the PA, COR/ACOR and the ECD APO Office at [redacted] For all excess property prior to taking any action. Excess personal property" means any personal property under the control of a Federal agency that the agency head determines is not required for its needs or for the discharge of its responsibilities.

20.3 Lost, Stolen, Damaged or Destroyed (LDD) property

- Unless otherwise provided in the contract, the contractor is liable for LDD of contract property, except for reasonable wear and tear in accordance with the contract's government property clause.
- Any occurrence of LDD must be investigated and fully documented by the PA and/or COR, who will promptly notify the CO. The contractor will submit a report of any incident of LDD contract property to the PA in accordance with the contract's government property clause and as detailed below, as soon as it becomes known.
- When GFP or CAP property is LDD, the Contractor must report within 24 hours of discovery of the event to the COR who will initiate a Report of Survey. This document will be obtained from ECD APO Office at [redacted]
- A Report of Survey will be prepared, regardless of whether or not preliminary research of an LDD event indicates positive evidence of negligence, misconduct, or unauthorized use and the responsible individual refuses to admit pecuniary liability.
- The Contractor must forward this document with all supporting documentation to the PA or COR within 5 business days of the LDD event for review.
- The PA and/or COR must submit the completed package to [redacted] within 5 business days of receipt from the Contractor.
- Contractor, PA and/or COR must supply all requested information and any

subsequent requests for information.

21.0 INVOICES

INVOICES AND PAYMENT PROVISIONS

Invoices shall be prepared per included FAR clauses. 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) Contract Line Item Number (CLIN) and Accounting Classifications
7) CLIN and description for each billed item.
8) Any additional backup information as required by this contract (to include the name/title of contractor support personnel billed against each CLIN).
9) ATTN: CISA/ECD

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

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.

22.0 CONTRACT ADMINISTRATION

Contracting Officer (CO):

The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds. The technical administration of this task order shall not be construed to authorize the revision of the terms and conditions of this task order. Any such revision will be authorized in writing by the Contracting Officer.

The Contracting Officer is the only person authorized to issue modifications to the contract, approve changes in any of the requirements, or obligate funds. Notwithstanding any clause/provision contained elsewhere in this contract, the authority to modify the contract remains solely with the Contracting Officer. If the Contractor makes any contract changes at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the contract to cover any increases in charges that may result. The Contracting Officer has the authority to perform any and all post-award functions in administering and enforcing the contract in accordance with its terms and conditions.

Name:	[redacted]
Agency:	Department of Homeland Security Cybersecurity and Infrastructure Security Agency
Telephone:	[redacted]
E-mail:	

Contract Specialist (CS):

The contract specialist performs duties as assigned by the CO. While the CO is ultimately responsible for negotiating and awarding contract actions, the contract specialist supports the CO extensively in the performance of his/her responsibilities. While the COR serves as the eyes and ears of the CO on his/her assigned contract(s), the contract specialist will likely be the person most accessible to COR in responding to COR requests for guidance and/or assistance. The contract specialist will also likely be the person that the COR can go to, to quickly escalate issues for CO attention and action.

Name:	[redacted]
Agency:	Department of Homeland Security Cybersecurity and Infrastructure Security Agency
Telephone:	[redacted]
E-mail:	

COR/ ACORs

The Contracting Officer has designated the COR/ACOR to assist in monitoring the work under this task order. The COR is responsible for the administration of the task order and technical liaison with the Contractor. The COR IS NOT authorized to change the scope of work or specifications as stated in the contract, to make any commitments or otherwise obligate the Government or

authorize any changes which affect the contract cost/price, delivery schedule, period of performance or other terms or conditions.

Name:	[redacted]
Agency:	Department of Homeland Security Cybersecurity and Infrastructure Security Agency
Telephone:	[redacted]
E-mail:	

Name:	[redacted]
Agency:	Department of Homeland Security Cybersecurity and Infrastructure Security Agency
Telephone:	[redacted]
E-mail:	

Name:	[redacted]
Agency:	Department of Homeland Security Cybersecurity and Infrastructure Security Agency
Telephone:	202-823-3752
E-mail:	[redacted]

23.0 IT Security

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 2.2, August 22, 2018 for TS SCI/C-LAN.

Supplemental Clauses
The following clauses, terms and conditions are incorporated with the same force and effect as if they were given in full text. Upon request, the contracting officer will make full text available.
The full text of a FAR clause may be accessed electronically at https://www.acquisition.gov/browse/index/far.
The full text of a DHS clause may be accessed at https://www.acquisition.gov/hsar.

All Applicable and Required provisions/clauses set forth in FAR 52.301 automatically flow down to all HCaTs task orders, based on their specific contract type (e.g. cost, fixed price, etc.), statement of work, competition requirements, commercial or not commercial, and dollar value as of the date the task order solicitation is issued. Representation and Certification Provisions from the HCaTs master contracts automatically flow down to all HCaTs task orders.

FAR Optional and Agency specific Task Order Provisions/Clauses. The following additional provisions and clauses apply to this task order.

52.216-31 Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition (Nov 2021)
52.217-5 Evaluation of Options (July 1990)
52.232-7 Payments under Time-and-Materials and Labor-Hour Contracts (Nov 2021)

52.204-23 PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB COVERED ENTITIES

(DEVIATION 20-05) (JUL 2024)

(a) *Definitions.* As used in this clause-

Kaspersky Lab covered article means any hardware, software, or service that–

(1) Is developed or provided by a Kaspersky Lab covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a Kaspersky Lab covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a Kaspersky Lab covered entity. *Kaspersky Lab covered entity* means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab, including any change in name, e.g., "Kaspersky";

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any Kaspersky Lab covered article. The Contractor is prohibited from—

(1) Providing any Kaspersky Lab covered article that the Government will use on or after October 1, 2018; and

(2) Using any Kaspersky Lab covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement.*

(1) In the event the Contractor identifies covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report, in writing, via email, to the Contracting Officer, Contracting Officer's Representative, and the Enterprise Security Operations Center (SOC) at [redacted], with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Enterprise SOC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 3 business days from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a Kaspersky Lab covered article, any reasons that led to the use or submission of the Kaspersky Lab covered article, and any additional efforts that will be incorporated to prevent future use or submission of Kaspersky Lab covered articles.

(d) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

(End of clause)

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (DEVIATION 20-05) (DEC 2020)

(a) *Definitions.* As used in this clause

"Backhaul" means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means

(l) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of2018 (50 U.S.C. 4817).

"Interconnection arrangements" means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

"Reasonable inquiry" means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

"Roaming" means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.*

(1) Section 889(a)(l)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(l)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) *Exceptions.* This clause does not prohibit contractors from providing-

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) *Reporting requirement.*

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause in writing via email to the Contracting Officer, Contracting Officer's Representative, and the Network Operations Security Center (NOSC) at NDAA [redacted] with required information in the body of the email. In the case of the Department of Defense, the Contractor shall report to the website athttps://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the NOSC, Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) and Contracting Officer's Representative(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.clod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(l) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

52.217-7 Option for Increased Quantity-Separately Priced Line Item (Mar 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within *30 days.* Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of clause)

52.217-8 Option to Extend Services (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the

Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within *30 days*.

(End of clause)

52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 3 years.

(End of clause)

52.224-3 Privacy Training – Alternate I (DHS DEVIATION 17-03)

(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)

3052.212-70 Contract Terms & Conditions Applicable to DHS Acquisition of Commercial Items (MAR 2023)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference

(a) *Provisions.*

(b) *Clauses.*

_X_ 3052.203–70 Instructions for Contractor Disclosure of Violations.

X_ 3052.204–71 Contractor Employee Access.

_X_ Alternate I

_X_ 3052.205–70 Advertisement, Publicizing Awards, and Releases.

_X_ 3052.209–72 Organizational Conflicts of Interest.

X_ 3052.215–70 Key Personnel or Facilities.

_X_ 3052.242–72 Contracting Officer's Representative.

(End of clause)

3052.215 -70 Key Personnel or Facilities (DEC 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel under this Contract:

Project Manager

(End of clause)

3052.204-71 CONTRACTOR EMPLOYEE ACCESS (JULY 2023)

(a) *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, 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.

(b) *Information Resources* means information and related resources, such as personnel, equipment, funds, and information technology.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted or subject to other investigations as required. All Contractor employees requiring recurring access to government facilities or access to CUI or information resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

(f) The Contractor shall include this clause in all subcontracts at any tier where the subcontractor may have access to government facilities, CUI, or information resources.

(End of clause)

ALTERNATE I (JULY 2023)

When the contract will require Contractor employees to have access to information resources, add the following paragraphs:

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

(h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract

award shall also be reported to the Contracting Officer.

(End of clause)

3052.204-72 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);
(vi) Contract clearance level;
(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)

HSAR 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)

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)