U.S. Department of Homeland Security
Office of Procurement Operations
Science and Technology Directorate
Diversity, Equity, Inclusion, and Accessibility Professional Support Services
Statement of Work (SOW)

1.0 Introduction

The objective of this acquisition is to acquire professional services to assist the Department of Homeland Security (DHS), Science and Technology Directorate (S&T) in the furtherance of establishing and maturing a Diversity, Equity, Inclusion and Accessibility Program that aligns with overarching Federal Government and Departmental directives. Support will include: program execution and planning; research and analysis; reporting; training; communications; and outreach and engagement.

2.0 Background

The Science and Technology (S&T) Directorate is the research and development arm of the Department of Homeland Security. The S&T Directorate is comprised of approximately 500 federal employees and 1000 contract support personnel disbursed across several geographically disjointed locations with its headquarters in Washington, D.C. The Directorate's Diversity, Equity, Inclusion, and Accessibility (DEIA) Office was established in July of 2022 and falls under the Office of Enterprise Services. Professional services acquired through this acquisition will support the full range of activities/tasks required to establish and mature a successful DEIA Office that executes in the spirit of Executive Order (EO) 14035 and other relevant EOs and higher headquarters guidance.

3.0 Applicable Documents

3.1 Reference Documents

- Executive Order 14035 Diversity, Equity, Inclusion, and Accessibility
- Government wide, strategic plan to advance, diversity, equity, inclusion, and accessibility in the federal workforce (Nov 2021)
- Office of Personnel Management Strategic Plan
- DHS Inclusive Diversity Strategic Plan
- Executive Order 13985 Advancing Racial Equity

4.0 Scope

The Contractor shall provide qualified personnel to perform the full range of human capital and programmatic services needed to support the DEIA Office. Core competencies needed to excel in this new office include:

technical competence in DEIA; investigative/diagnostic information gathering and analysis; performance measurement; technologically savvy; results oriented; environmental awareness (organizational, political, and societal); effective communication; interpersonal mastery; stakeholder management; and attention to detail. These core competencies will be used to accomplish the following:

4.1 Program Planning and Execution - Primary Contractor services for Program Planning and Execution shall be:

4.1.1 The Contractor shall support strategic planning in the implementation of both mature and innovative solutions to S&T DEIA weaknesses and opportunities and the integration of DEIA considerations and proven/promising practices into existing strategies and operations across the organization.

4.1.1.1 The Contractor shall facilitate the development of a five (5) year DEIA strategy that aligns with Federal, Departmental, and Directorate guidance and goals. The strategy shall aim to incorporate higher headquarter guidance and goals while also presenting strategies to eliminate S&T specific organizational barriers and weaknesses and establish organizational metrics to track progress.

4.1.1.2 The Contractor shall facilitate the development of annual action plans that align to the strategic plan. Annual action plans shall be developed and presented for consideration and adoption no later than 1 September of each fiscal year.

4.1.1.2.1 The action plan shall address any emerging/dynamic environmental considerations that have arisen since the publication of the strategic plan.

4.1.1.2.2 The action plan shall take into account outcomes from previous years to improve performance and outcomes for the DEIA Office.

4.1.1.2.3 The action plan shall reflect distinct actions for Diversity, Equity, Inclusion, and Accessibility. Actions may also support multiple focus areas.

4.1.1.2.4 The contractor shall develop and deliver a detailed logic model and theory of change in support of the developed action plan. The logic model shall include activities, required resources, outputs, and the resulting positive outcomes associated with organizational goals.

4.1.1.3 The Contractor shall support the integration of DEIA considerations into other organizational strategies that fall outside the purview of the DEIA Office. These strategies include but are not limited to: Strategic Recruitment and Retention; Performance Management; Employee Engagement: Minority Serving Institutions (MSI) Engagement; and Small Business Outreach.

4.1.1.4 The Contractor shall collaborate effectively with DEIA, HR and EEO practitioners and key stakeholders across the agency to seek guidance and support as necessary to prepare strategic and action plans.

4.1.1.5 The Contractor shall support the implementation and management of initiatives flowing from the approved Directorate action plan. The contractor shall utilize automation and data visualization tools to establish readily available data dashboards that reflect organizational progress towards DEIA metrics and goals throughout the period of performance.

4.1.1.6 The Contractor shall facilitate no less than two (2) webinars or in-person events each year to highlight annual initiatives as outlined in the action plan to the Directorate workforce.

4.1.1.7 The contractor shall facilitate the development of a DEIA Office Program Management Plan (PMP) in accordance with the Science and Technology Directorate PMP template. A draft PMP shall be completed within 90 days of contract award. The PMP shall serve as a continuity document for the office and shall be updated as significant changes occur during the period of performance of this contract.

4.1.2 The Contractor shall support day-to-day operations of the DEIA Office

4.1.2.1 The Contractor shall attend and contribute to internal office meetings to ensure synchronization and synergy in successfully accomplishing Office tasks. The Contractor shall capture meeting notes and upload to team collaboration platform.

4.1.2.2 The Contractor shall attend and capture notes and action items during meetings with external stakeholders to ensure synchronization and synergy. Deliver meeting minutes/notes to meeting attendees within two (2) business days.

4.1.2.3 The Contractor shall monitor and respond appropriately to incoming correspondence/requests for support via the DEIA mailbox. Responses, final or interim, shall occur within 4 hours of receipt.

4.1.2.3.1 The contractor shall facilitate the timely delivery of reasonable accommodations procurement requests received by the DEIA office.

4.1.2.3.2 The contractor shall maintain an accounting of all requests for support and level of effort required for requests.

4.1.2.4 The Contractor shall monitor and close out tasks assigned to the DEIA Director and/or the DEIA office in the directorate's executive secretariat task tracking system prior to suspense date. A proposed draft response shall be provided to the DEIA Director no less than 1 business day prior to the suspense date for clearance.

4.1.2.5 The Contractor shall use online reservation applications and other productivity tools to facilitate the efficient scheduling of onsite meetings and engagements. Meeting attendees shall receive meeting materials no later than 1 business day prior to scheduled engagements.

4.1.2.6 The Contractor shall use the directorate's travel management system to schedule/book travel for the DEIA Office. Travel booking shall be executed within 2 business days of notification of travel by the Government.

4.1.2.7 The Contractor shall collaborate effectively with DEIA, HR and EEO practitioners and key stakeholders across the agency to leverage resources and ensure organizational synergies. The contractor shall seek guidance and support as necessary to execute tasks through participation in working groups/task forces and through direct engagement.

4.1.2.8 The Contractor shall develop and publish Standard Operating Procedures (SOPs) to codify any new internal office procedures or overarching Directorate DEIA procedures.

4.1.2.9 The Contractor shall maintain a DEIA Teams channel that serves as a collaboration platform and repository for internal team documents.

4.2 Research and Analysis - Primary Contractor services for Research and Analysis shall be:

4.2.1 The Contractor shall maintain continued awareness of the internal and external DEIA environment to include legislation, policy, research, and reports. The contractor shall identify reputable sources to seek new DEIA topics and alert the DEIA Director of substantive information no less than weekly.

4.2.2 The Contractor shall research and analyze DEIA focus areas based on Executive Order guidance and internal priorities to make recommendations on requisite actions to address disparities, gaps, and/or weaknesses.

Data shall be pulled from appropriate HR data systems in coordination with higher headquarters human capital and EEO offices.

4.2.2.1 The Contractor shall conduct organizational workforce health assessments through interviews, demographic data analysis, and surveys to assess organizational climate (to include employee perceptions), barriers to DEIA, and organizational performance in meeting DEIA goals. The Contractor shall adhere to Government and/or industry standards and best practices in execution of this task.

4.2.2.2 The Contractor shall conduct organizational equity assessments through data analysis and surveys. The Contractor shall adhere to Government and/or industry standards and best practices in execution of this task.

4.3 Reporting - Primary Contractor services for Reporting shall be:

4.3.1 The Contractor shall produce executive-level reports, briefs, and/or papers on internal and external DEIA focus areas and trends to promote organizational awareness and accountability through data storytelling. Reports/briefs shall include the findings and summation of the organizational workforce health and equity assessments (4.2.2.1 and 4.2.2.2)

4.3.2 The Contractor shall produce quarterly reports that capture organizational accomplishments in DEIA for the previous quarter. Reports will be in accordance with higher headquarters templates and/or Directorate guidance.

4.3.3 The Contractor shall produce an executive-level annual report that includes compelling data storytelling and graphical representations in capturing organizational accomplishments for the year. Data from the report shall also be reformatted and used to support annual Departmental reporting to the White House in support Executive Order tracking.

4.3.4 The Contractor shall produce monthly reports to highlight Contractor accomplishments and to support contract billing. This report shall capture efforts for the prior month and shall also be represented graphically to reflect workload and service request trends. Reports shall be delivered to the Government no later than five (5) days after the start of each month.

4.3.5 The Contractor shall produce weekly email summaries of significant team accomplishments, challenges, trending topics (as described in 4.1.2.10 and 4.2.1.1). Contractor team leave and coverage information for the following week shall be included.

4.4 DEIA Training - Primary Contractor services for DEIA Training shall be:

4.4.1 The Contractor shall develop and manage an annual DEIA training and awareness schedule in accordance with the annual action plan. The training schedule shall he designed to support employees, managers, leadership, and in some cases Contractor personnel. The proposed training schedule shall leverage relevant speakers, researchers, and private/public organizations that have a significant body of work to contribute meaningfully to DEIA discussions, webinars, and events. No fewer than six (6) sessions shall be proposed per year.

4.4.2 The Contractor shall develop and deploy post-training surveys to assess effectiveness of DEIA training in meeting intended outcomes. Surveys shall be deployed no later than 1 day following the training event. Survey data shall be compiled and maintained for reporting purposes.

4.5 Communications and Outreach - Primary Contractor services for Communications Online Presence And Resource Repository Support shall be:

4.5.1 The Contractor shall develop and execute a communications plan aligned with DEIA principles and plans to address organizational needs in a diplomatic, alliance-building manner. Communications shall be without grammatical errors and editorial issues 95% of the time. The Contractor shall perform quality control of broad disseminations to the workforce.

4.5.1.1 The Contractor shall produce and present for release monthly communications that are relevant, timely and keep DEIA principals and initiatives at the forefront of the organization. The Contractor shall produce no less than two (2) communications for Directorate-wide dissemination per month.

4.5.1.2 The Contractor shall produce and present for release no less than two (2) communications that promote observances of departmental special emphasis programs. The Contractor shall also collaborate with the S&T Communications and Outreach Division to incorporate special emphasis observances in other S&T publications.

4.5.1.3 The Contractor shall develop and present a DEIA Overview Brief during all S&T Orientation/Onboarding sessions throughout the year.

4.5.1.4 The Contractor shall ensure all communications and outreach materials are 508 compliant (defined below in 6.17) to facilitate user accessibility. The Contractor shall use appropriate desktop publishing applications/tools to ensure compliance. All distributed materials shall be in compliance and be delivered in advance of briefings and/or presentations when applicable.

4.5.2 The Contractor shall lead facilitation of DEIA Office council sessions to include scheduling, logistics, and meeting management and follow-up actions. The Contractor shall work with council members to ensure progress on council goals and objectives.

4.5.2.1 The Contractor shall support the chartering and management of any S&T established Employee Resource Groups (ERGs). Track ERG engagement assess the impact of outreach.

4.5.2.2 The Contractor shall develop marketing and outreach materials to be used during recruitment and engagement events. Ensure materials maintain DEIA and S&T branding. Collaborate with COD for support and quality control as necessary.

4.6 Online Presence and Resource Repository - Primary Contractor services for Online Presence And Resource Repository Support shall be:

4.6.1 The Contractor shall lead the development and maintenance of a DEIA website and SharePoint site as a resource tool for managers, employees, and potential employees, contractors, or industry partners

4.6.1.1 The Contractor shall leverage data storytelling to provide transparency surrounding S&T demographic data

4.6.1.2 The Contractor shall maintain a repository of relevant policy documents, strategies, research, reports, articles, and other information resources that are relevant to employees and supervisors on the internal SharePoint site.

4.6.1.3 The Contractor shall include various types of media on the DEIA external site to maintain user engagement.

4.6.1.4 The Contractor shall track and provide data on the use of online resources.

4.6.1.5 The Contractor shall establish actions and strategies to maintain DHS staff engagement with online DEIA materials and resources

4.6.1.6 The Contractor shall establish and maintain consistent DEIA Office branding across all online platforms.

4.6.1.7 The Contractor shall ensure all online and SharePoint content is 508 compliant to support user accessibility. All documents uploaded and/or posted to DEIA repositories shall also be 508 compliant for user accessibility.

5.0 DELIVERABLES

5.1 All documents produced under this PWS shall be created in Microsoft Word, Microsoft Project, Microsoft PowerPoint or Microsoft Excel, Microsoft Access, and other compatible Windows software and Department of Homeland Security – S&T systems as approved by the COR. The COR may request that documents be delivered in hard copy and / or electronic copy format. All Contractor electronic deliverables shall be 508 compliant.

5.1.1 Post Award Conference. The Contractor shall attend a Post Award Conference with the Contracting Officer, COR, and DEIA Director 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 Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held via video teleconference.

5.1.2 Transition-In Plan. The transition-in phase shall be in accordance with the Contractor's written submitted Transition-In Plan. The Transition-In Plan shall consist of the Contractors plan for minimizing impact such that the continuity of services will be maintained without disruption and describe how it will achieve full staff support levels within 60 days of award.

The Transition-In Plan shall be submitted within 14 days of Task Order award to the CO and COR. The Transition-In Plan will be reviewed by the COR and feedback will be provided within seven (7) days from the date of Contractor submission. If the feedback provided by the COR specifies that corrections shall be made to the deliverable, the Contractor shall resubmit the deliverable(s) within seven (7) days from the date comments/feedback are received.

The Transition-In Plan shall be consistent with the Transition-In Approach presentation and supporting slides as submitted with the Contractor's Factor 3 Oral Presentation submission.

The Government will provide the Contractor office space and telephone access for required on-site personal. The phase-in transition period shall begin at date of contract award and shall conclude 60 days later. Upon completion of the phase-in transition period, the Contractor shall assume full operating accounting and responsibility. The transition-in period may be extended in order to ensure an orderly draw down of outgoing personnel and ramp up of incoming personnel.

5.1.3 Transition-Out Plan. The transition-out phase shall be in accordance with the Contractor's submitted Transition-out Plan. The Transition-out Plan shall address the Contractor's plan for minimizing impact such that continuity of services will be maintained without disruption. The Contractor shall describe how it will transition work to the new Contractor.

The Transition-out Plan shall be submitted 180 days before the expiration of the period of performance to the CO and COR. If the feedback provided by the COR specifies that corrections shall be made to the deliverable, the Contractor shall resubmit the deliverable(s) within seven (7) days from the date comments/feedback are received.

5.1.4 Project Plan. The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 14 business days after the Post Award Conference.

5.1.5 Monthly Progress Reports. The Contractor Manager shall provide a monthly progress report to the CO, COR, and DEIA Director via electronic mail. This report shall provide monthly cost and performance reporting of all assigned tasks. The costs portion of the report shall be structured to enable ready discernment of cost trends, projections, and variances. At a minimum these reports shall include:

Technical Information:

- All Contractor work performed and planned to be performed, i.e., a list of planned activities, activities in progress, and completed activities for each support staff performing under the task order.
- An assessment of technical progress.
- Identification of any problem areas with each assigned task.
- Any major issues affecting performance and expected to affect performance.
- Schedule for any assigned work; and
- Any other Contractor concerns or recommendations.

Cost Information

- Total amount funded on the task order
- Current and cumulative expenditures per task to date, including breakdown of labor by hours by labor category, applied indirect expenses, all other direct costs, and costs for any travel conducted.
- Any planned travel and anticipated costs.
- Any major issues affecting cost.
- Projected expenditures for the next reporting period and to term; and
- Graphical spending charts and metrics to assess costs, schedule, and technical performance.

5.1.6 Trip Summary Report. The Contractor shall provide trip summary reports of any trip taken in support of this contract. The trip summary report shall include travel purpose, a list of persons contracted while on travel, a summary of all meetings/events attended, and any relevant documents.

The report shall be submitted via electronic mail to the COR and CO no later than five working days from the last day of travel.

5.1.7 Progress Meetings. The Contractor shall meet with the COR on a bi-weekly basis to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place via teleconference.

Actionable Deliverable Due	SOW Reference	Deliverable Due Date	Distribution
Develop a five (5) year DEIA strategy	4.1.1.1	150 calendar days after award	PM
Develop annual action plans	4.1.1.2	90 calendar days after award and thereafter Annually Not Later Than September 1	PM
Develop and Deliver Logic Model and Theory of Change	4.1.1.2.4	90 calendar days after award and thereafter Annually Not Later Than September 1	PM
Establish Readily Available Data Dashboards	4.1.1.5	60 calendar days after the delivery of annual action plan	PM
Facilitate no less than two (2) annual DEIA goals webinars	4.1.1.6	TBD but no later than 60 calendar days after action plan release	PM
Develop Draft DEIA Program Management Plan	4.1.1.7	90 calendar days after contract award	PM
Develop and Publish Standard Operating Procedures	4.1.2.8	no more than 30 calendar days from request	PM
Conduct Workforce Health Assessment	4.2.2.1	Upon request but no less than once during each year of POP	PM
Conduct Organizational Equity Assessment	4.2.2.2	Upon request but no less than once during each year of POP	PM
Produce executive-level reports	4.3.1	Upon request	PM
Produce Quarterly Progress Reports	4.3.2	Not later than 15 business days following	PM/COR

		the close of each fiscal quarter	
Produce Executive-level Annual Report	4.3.3	No later than 10 business after the close of each fiscal year	PM
Produce monthly reports	4.3.4	5 calendar days after the close of each month IAW 6.1.5	PM/COR
Produce weekly email summaries	4.3.5	Every Friday No Later than Close of Business	PM
Develop and Manage Annual DEIA Training and Awareness Schedule	4.4.1	No later than one month after the delivery of the annual action plan	PM
Develop and Deploy Post-Training Surveys	4.4.2	No later than 1 day following the training event	PM
Develop and execute a communications plan	4.5.1	No later than 90 calendar days after contract award	PM
Produce and present for release monthly communications	4.5.1.1	As requested	PM
Produce and present for release no less than two (2) special emphasis communications	4.5.1.2	As required	PM
Develop and Present DEIA Overview Brief for New Employee Orientation	4.5.1.3	90 calendar days after contract award	PM
Develop Marketing and Outreach Materials	4.5.2.2	As requested	PM
Post Award Conference	5.1.1	Not Later Than 10 business days after award	OPO/PM/COR
Transition-In Plan	5.1.2	within 14 calendar days of Task Order award	PM/COR
Transition-Out Plan	5.1.3	180 calendar days before the expiration of the period of performance	PM/COR

Final Project Plan	5.1.4	14 calendar days after award	OPO/PM/COR
Monthly Progress Report **(Same report as 4.3.4)**	5.1.5	Not later than the fifth calendar day of each month	COR/PM
Trip Summary Report	5.1.6	5 calendar days upon completion	COR/PM
Progress Meeting	5.1.7	Bi-weekly	COR/PM

6.0 Other Applicable Conditions

6.1 Period of Performance

The period of performance for this contract is a one-year base period with four one-year option periods.

Base Period	09/30/2023 – 09/29/2024
Option Period One	09/30/2024 – 09/29/2025
Option Period Two	09/30/2025 – 09/29/2026
Option Period Three	09/30/2026 – 09/29/2027
Option Period Four	09/30/2027 – 09/29/2028

The Contractor will not work on the following Federal Holidays when the DHS S&T facility is closed:

January 1	New Year's Day
Third Monday in January	Birthday of Martin Luther King, Jr.
Third Monday in February	Washington's Birthday
Last Monday in May	Memorial Day
June 19th	Juneteenth
July 4	Independence Day
First Monday in September	Labor Day
Second Monday in October	Columbus Day
November 11	Veterans Day
4th Thursday in November	Thanksgiving Day
December 25	Christmas

6.2 Employee Identification

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

Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

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

6.3 Employee Conduct

6.3.1 Contractor personnel shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

6.3.2 **Office Conduct.** Contractor must ensure contract staff are readily accessible and available to Government staff through MS Teams, e-mail, phone, an office visits during working hours. The Contractor shall provide contract teamwork hours to the DEIA Office Director.

6.4 Continuity Of Support. The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., the Contractor shall provide e-mail notification to the PM and Contracting Officer's Representative (COR) prior to employee absence. In all cases of planned employee absence, the Contractor shall provide a fully qualified replacement for the length of the planned absence due to vacation or leave.

6.5 Qualified Personnel. The Contractor shall provide qualified personnel to perform all requirements specified in this PWS.

6.6 Key Personnel. A Key Personnel resume is required for the Senior Management Analyst position and the Government shall have the opportunity to review the qualifications, education and experience of proposed Contractor personnel and approve individuals for work under this task order before their paperwork is submitted to Personnel Security for clearance.

6.6.1 Before replacing any Key Personnel, the Contractor shall notify the Contracting Officer at least 20 business days in advance, The Contractor must submit written justification for replacement and provide the resumes of proposed substitute(s) at that time. Proposed substitutes shall possess qualifications equal or superior to those of the Key Personnel being replaced. The Contractor shall not replace Key Personnel without the Contracting Officer's approval. The Government may designate any additional positions as Key Personnel at the time of award.

6.6.2 The Senior Management Analyst is further designated as Key Personnel by the Government. During any absence of the Senior Management Analyst, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. The Senior Management Analyst and all designated alternates shall be fluent in written and spoken English.

The Senior Management Analyst shall be available to the PM and COR via telephone between the hours of 8:00 A.M and 5:00 P.M. EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 3 hours of notification.

6.6.3 The below personnel are identified as key personnel:

LCAT: Senior Management Analyst – Eleanor Thomas

6.7 Removing Employees for Misconduct Or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer*), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

6.8 Telework. Regular/recurring telework may be authorized by the PM and COR for this contract. The rates charged shall be the same as the government site rate in effect under this contract for the relevant period(s) of performance.

Contractor employees will be required to provide a telework plan within 10 days after contract award or after 90 days when an individual begins work on the contract. A situational telework plan shall be in effect for situational (ad hoc) telework to be approved by the COR before each occurrence. A telework plan may be revised at the Government's discretion. The contractor shall receive approval for situational telework from the COR before entering telework status.

6.9 Replacing Individuals. The Contractor shall submit complete and correct information to DHS's Personnel Security Division for new personnel to backfill a position within ten days of notifying the Government of the previous personnel's last day.

6.10 DHS-Furnished Information. DHS will provide DHS information, materials, and forms unique to DHS to the Contractor to support tasks under this PWS. Such DHS-provided information, materials, and forms shall remain the property of DHS, unless otherwise indicated in writing by DHS, and may not be distributed beyond the Contractor project performers without DHS's prior written permission.

6.11 Place Of Performance The primary place of performance will be the Department of Homeland Security, Science and Technology Directorate facilities. Specific location within the DC metro area will be determined at a later date.

6.12 Invoices. Invoices should be submitted monthly to Invoice[redacted] with copies to the Contracting Officer and Contracting Officer's Representative (COR).

6.13 Security. Contractor access to unclassified, but Security Sensitive Information may be required under this PWS. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

DHS has determined that the performance of this contract requires a Public Trust suitability clearance before an individual can begin work under the contract. Upon official notification by the Government that a clearance will not be granted, the contractor shall provide the security paperwork for a qualified replacement within thirty calendar days.

DHS may exercise full control over granting, denying, withholding, or terminating unescorted access to DHS facilities, DHS systems, and/or sensitive DHS information for Government/Contractor employees. Access will be based upon the results of a DHS fitness/suitability investigation. DHS may, as appropriate, make favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the Government/Contractor employee to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full DHS fitness/suitability authorization will follow. The granting of a favorable EOD decision or a full DHS fitness/suitability authorization determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the contract/task order. No employee of the Government/Contractor shall be allowed unescorted access to a DHS facility, access to any sensitive DHS information, or access to DHS Systems without a favorable EOD decision or DHS fitness/suitability determination by the DHS HQ Office of Security. Government/Contractor employees assigned to the contract/task order not needing access to sensitive DHS information, DHS systems, or access to DHS facilities will not be subject to DHS fitness/suitability screening. Government/Contractor employees waiting on an EOD decision may not begin work on the contract. Limited access to DHS facilities is allowable prior to the EOD decision if the Government/Contractor employee is escorted by an approved DHS employee. This limited access is to allow Government/Contractor employees to attend briefings, nonrecurring meetings, and begin transition work.

During one's limited access the Government/Contractor employee will not have access to sensitive or classified DHS information.

The Contractor shall adhere to all applicable Government laws, regulations, orders, guides, and directives pertaining to classified, Sensitive But Unclassified (SBU), FOUO, or personally identifiable information. The Contractor shall safeguard SBU, FOUO information specifically in accordance with DHS Management Directive 11042.1 and in compliance with HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information. Email notification shall state the required training has been completed for all Contractor and subcontractor employees.

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

6.15 Travel. Local, Domestic, and/or international travel may be required for this contract. Any local travel within 50 miles of an individual's normal duty location will not be reimbursed.

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

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

6.17 Section 508 Compliance. Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

6.18 Data Rights. Refer to FAR 52.227-14 Addendum – Private Use of Data First Produced at Section 12.0 of the Terms and Conditions.

6.19 Release of Information. If Contractor and its personnel have access to Personally Identifiable Information (PII), Classified Information, and other controlled unclassified information (CUI) which is not releasable to the general public, the Contractor or its personnel shall not release any information or documents that they are provided during performance of the contract without the express written permission of the CO through coordination with the COR.

6.20 Government Furnished Resources. 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 Performance Work Statement.

No Government Furnished information such as manuals, drawings, test data, etc. will be provided to prospective contractors bidding on this work.

6.21 Administration of Government Property

1. Pursuant to the clause of this contract Government Property, FAR 52.245-1, the Contractor shall be accountable to DHS for personal property (1) provided by DHS as Government Furnished Equipment (GFE); or (2) that is Contractor Acquired Property (CAP) acquired with DHS funds where (a) the CAP has an acquisition cost of $5,000 or more or (b) where the CAP is sensitive assets of any value, defined as laptops, cameras, Ironkeys, and any other property that may have retainable storage memory.

2. The Contractor shall provide a listing of all GFE or CAP to the DHS Contracting Officer annually on the anniversary date of this Contract.

3. Ninety (90) days prior to the completion of work and acceptance of all deliverables under this Contract, the Contractor shall provide the DHS Contracting Officer the final and complete listing of all GFE and CAP charged to this Contract with an acquisition cost of $5,000 or more or sensitive assets.

4. The DHS Contracting Officer will provide Contractor with instructions for disposition of all GFP and CAP and provide any additional funds to enable that disposition, as necessary.

7.0 Government Terms & Definitions

COR – Contracting Officer's Representative
DHS - Department of Homeland Security
HSE – Homeland Security Enterprise
IDIQ – Indefinite Delivery, Indefinite Quantity
OES - Office of Enterprise Services
OPO – Office of Procurement Operations
S&T - Science and Technology Directorate
SOW – Statement of Work

TA – Travel Authorization
T&M – Time and Materials
DEIA – Diversity, Equity, Inclusion & Accessibility

8.0 Government Acceptance Period

The COR will review deliverables prior to acceptance and provide the Contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

8.1 The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

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

8.3 All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

9.0 POINTS OF CONTACT

9.1 Contractor Points of Contact (POC) – TBD

9.2 Government (DHS) POCs

DHS IDIQ Task Order Contracting Officer

[redacted]

DHS IDIQ Task Order Contract Specialist

[redacted]

DHS Task Order Contracting Officer Representative

[redacted]

DHS S&T Project Manager

[redacted]

DHS S&T may change the individual designated as a POC upon notice to the Contractor of such change.

GS02Q16DCR0109 / 70RSAT23FR0000139
Diversity, Equity, Inclusion, and Accessibility (DEIA) Office Professional Support Services
U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T)

Terms and Conditions

Issued Under:
GSA's Human Capital and Training Solutions (HCaTS)
Indefinite-Delivery, Indefinite-Quantity (IDIQ) Contract

1.0. HCATS TASK ORDER GENERAL INFORMATION

HCaTS Vehicle: HCaTS Small Business

HCaTS Pool: Small Business Pool 2 (NAICS 541611 – Administrative Management and General Management Consulting Services)

Requirement Title: Diversity, Equity, Inclusion, and Accessibility (DEIA) Office Professional Support Services

Issuing Office: U.S. Department of Homeland Security
Office of Procurement Operations
Science and Technology Acquisitions Division

2.0 TASK ORDER CONTRACT INFORMATION

2.1. NAICS Code and Small Business Size Standard: The principal nature of the requirements described in this solicitation is consistent with services performed by industries in the NAICS Code 541611 – Administrative Management and General Management Consulting Services with a small business size standard of $24.5M.

2.2. Product Service Code (PSC): The services in this solicitation are best represented by PSC Code: R408 Support – Professional: Program Management/Support

2.3. Type of Contract: The primary type of contract resulting from this solicitation is: Time-and-Materials (T&M)

2.4. Type of Services: The type of services under this solicitation is:

☒ Commercial Items ☐ Non-Commercial Items ☐ Mix of Both

2.5. Extent of Competition: This solicitation will be based on:

2.5.1. ☒ Fair opportunity procedures (FAR 16.505(b)(1))

2.6. Security Clearances:

2.6.1. The clearance level for this SOW is:
☒ Unclassified ☐ Classified ☐ Mix of Both

2.7. Performance Location(s):

2.7.1. The performance locations for this SOW are:
☒ CONUS ☐ OCONUS ☐ Mix of Both

2.7.3. The labor will be performed at:
☒ Government Site ☐ Contractor Site ☐ Mix of Both

2.8. Place(s) of Performance:

2.8.1. The places of performance(s) for this SOW are:

The primary place of performance will be the Department of Homeland Security, Science and Technology Directorate facilities. Specific location within the DC metro area will be determined at a later date.

2.9. Period of Performance:

2.9.1. The period of performance for this SOW is:

Base Period	09/30/2023 – 09/29/2024
Option Period One	09/30/2024 – 09/29/2025
Option Period Two	09/30/2025 – 09/29/2026
Option Period Three	09/30/2026 – 09/29/2027
Option Period Four	09/30/2027 – 09/29/2028

See Statement of Work, Section 6.1.

2.10. Kickoff Meeting:

Kickoff meeting information will be provided at award.

3.0 CONTRACT LINE ITEMS (CLINS) AND CONTRACT TYPE

List of CLIN(s) and Sub-CLIN(s):

CLIN 0001	BASE LABOR
CLIN 0002	OPTIONAL SURGE LABOR
CLIN 0003	OTHER DIRECT COSTS
	TRAVEL NOT-TO-EXCEED $30,000.00
CLIN 0004	CAF (0.75%) - BASE PERIOD
CLIN 1001	OPTION YEAR 1 - LABOR
CLIN 1002	OPTION YEAR 1 – OPTIONAL SURGE LABOR
CLIN 1003	OPTION YEAR 1 - OTHER DIRECT COSTS
	TRAVEL NOT-TO-EXCEED $30,000.00
CLIN 1004	CAF (0.75%) – OPTION YEAR 1

CLIN 2001 OPTION YEAR 2 – LABOR
CLIN 2002 OPTION YEAR 2 – OPTIONAL SURGE LABOR
CLIN 2003 OPTION YEAR 2 – OTHER DIRECT COSTS
TRAVEL NOT-TO-EXCEED $30,000.00
CLIN 2004 CAF (0.75%) – OPTION YEAR 2

CLIN 3001 OPTION YEAR 3 - LABOR
CLIN 3002 OPTION YEAR 3 – OPTIONAL SURGE LABOR
CLIN 3003 OPTION YEAR 3 – OTHER DIRECT COSTS
TRAVEL NOT-TO-EXCEED $30,000.00
CLIN 3004 CAF (0.75%)- OPTION YEAR 3

CLIN 4001 OPTION YEAR 4 - LABOR
CLIN 4002 OPTION YEAR 4 – OPTIONAL SURGE LABOR
CLIN 4003 OPTION YEAR 4 – OTHER DIRECT COSTS
TRAVEL NOT-TO-EXCEED $30,000.00
CLIN 4004 CAF (0.75%) – OPTION YEAR 4

The multiple Optional CLIN(s) may be exercised by the Government unilaterally under FAR 52.217-7, per the Services and Price Schedule in this section.

4.0 DESCRIPTION OF SERVICES/SCOPE OF WORK

Please refer to the attached Statement of Work.

5.0 PERFORMANCE MANAGEMENT APPROACH

Please refer to the attached Statement of Work.

6. KEY PERSONNEL APPOINTMENTS

Please refer to the attached Statement of Work, Section 6.6.

7.0 DELIVERY AND PERFORMANCE INFORMATION

Please refer to the attached Statement of Work.

8.0 LABOR CATEGORIES AND DESCRIPTIONS

Please refer to the attached Statement of Work and Pricing Table.

9.0 RESERVED

10.0 NON-DISCLOSURE AGREEMENT (NDA)

Contractor access to proprietary information is required under the attached Statement of Work. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation, DHS MD 11042.1, Safeguarding

Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to personally identifying information, business, or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

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

11.0 INVOICING INSTRUCTIONS

Refer to the Statement of Work, Section 6.12.

12.0 TASK ORDER CLAUSES

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, 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. In addition, the following FAR clauses are hereby incorporated by reference:

FAR Clause No.	Title and Date
52.204-2	Security Requirements (Mar 2021)

12.1. FAR and Agency Specific Task Order Clauses. The following additional clauses apply to this task order:

Clauses

FAR 52.204-14 Service Contract Reporting Requirements (OCT 2016)

(a) Definition.

First-tier subcontract means a subcontract awarded directly by the Contractor for the purpose of acquiring supplies or services (including construction) for performance of a prime contract. It does not include the Contractor's supplier agreements with vendors, such as long-term arrangements for materials or supplies that benefit multiple contracts and/or the costs of which are normally applied to a Contractor's general and administrative expenses or indirect costs.

(b) The Contractor shall report, in accordance with paragraphs (c) and (d) of this clause, annually by October 31, for services performed under this contract during the preceding Government fiscal year (October 1-September 30).

(c) The Contractor shall report the following information:

(1) Contract number and, as applicable, order number.

(2) The total dollar amount invoiced for services performed during the previous Government fiscal year under the contract.

(3) The number of Contractor direct labor hours expended on the services performed during the previous Government fiscal year.

(4) Data reported by subcontractors under paragraph (f) of this clause.

(d) The information required in paragraph (c) of this clause shall be submitted via the internet at www.sam.gov. (See SAM User Guide). If the Contractor fails to submit the report in a timely manner, the contracting officer will exercise appropriate contractual remedies. In addition, the Contracting Officer will make the Contractor's failure to comply with the reporting requirements a part of the Contractor's performance information under FAR subpart 42.15.

(e) Agencies will review Contractor reported information for reasonableness and consistency with available contract information. In the event the agency believes that revisions to the Contractor reported information are warranted, the agency will notify the Contractor no later than November 15. By November 30, the Contractor shall revise the report, or document its rationale for the agency.

(f) (1) The Contractor shall require each first-tier subcontractor providing services under this contract, with subcontract(s) each valued at or above the thresholds set forth in 4.1703(a)(2), to provide the following detailed information to the Contractor in sufficient time to submit the report:

(i) Subcontract number (including subcontractor name and unique entity identifier); and

(ii) The number of first-tier subcontractor direct-labor hours expended on the services performed during the previous Government fiscal year.

(2) The Contractor shall advise the subcontractor that the information will be made available to the public as required by section 743 of Division C of the Consolidated Appropriations Act, 2010.

(End of clause)

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and ServicesDeveloped or Provided by Kaspersky Lab and Other Covered Entities (NOV 2021)

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

Covered article means any hardware, software, or service that–

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

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

(3) Contains components using any hardware or software developed in whole or in partby a covered entity.

Covered entity means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control withKaspersky 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 forFiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

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

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

(c) *Reporting requirement.*

(1) In the event the Contractor identifies a covered article provided to the Governmentduring contract performance, or the Contractor is notified of such by a subcontractor at any tieror any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders inthe 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 1 business day from the date of such identification or notification: thecontract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesalernumber); 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 orsubmission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission ofcovered articles.

(d) Subcontracts. The Contractor shall insert the substance of this clause, including thisparagraph (d), in all subcontracts including subcontracts for the acquisition of commercial products or commercial services.

(End of clause)

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications andVideo Surveillance Services of Equipment (Deviation 20-05) (NOV 2021)

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

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

Telecommunications or video surveillance services provided by such entitiesor using such equipment; or

Telecommunications or video surveillance equipment or services produced orprovided 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–

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

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 VIIof title 15, Code of Federal Regulations, and controlled-

Pursuant to multilateral regimes, including for reasons relating to nationalsecurity, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

For reasons relating to regional stability or surreptitious listening;

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);

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

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

Emerging and foundational technologies controlled pursuant to section 1758of the Export Control Reform Act of 2018 (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 offtraffic 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 otherinformation 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 toinclude an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) receivedfrom 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 properfunction or performance of a piece of equipment, system, or service.

Prohibition. (1) Section 889(a)(1)(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 extendingor 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)(1)(B) of the John S. McCain National Defense AuthorizationAct 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.

Exceptions. This clause does not prohibit contractors from providing—

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

Telecommunications equipment that cannot route or redirect user data trafficor permit visibility into any user data or packets that such equipment transmits or otherwise handles.

Reporting requirement. (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential componentof 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 thisclause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, theContractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case ofthe Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil. The Contractor shall report the following information pursuant to paragraph(d)(1) of this clause 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 undertakenor recommended.

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 orservices, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

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

(End of clause)

FAR 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 10 business days.

(End of clause)

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

The Government may extend the term of this contract by written notice to the Contractor within *7 days*; provided that the Government gives the Contractor a preliminary written noticeof its intent to extend at least *10 days* before the contract expires. The preliminary notice does not commit the Government to an extension.

If the Government exercises this option, the extended contract shall be considered to includethis option clause.

The total duration of this contract, including the exercise of any options under this clause, shall not exceed *60 months*.

(End of clause)

FAR 52.224-3 Privacy Training (Jan 2017) Alternate I (Jan 2017)

(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 StrategicResource).

(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 otherwisehandle 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 and39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy trainingthereafter, to Contractor employees for the duration of this contract.

(d) The Contractor shall maintain and, upon request, provide documentation of completion ofprivacy 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 operatea 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 subcontractsunder 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 otherwisehandle personally identifiable information; or Design, develop, maintain, or operate a system of records

FAR 52.227-14 Rights in Data—General (May 2014)

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

"Computer database" or "database means" a collection of recorded information in a form capableof, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"—

(1) Means

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specificoperation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes,flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation. "Computer software

documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, thatexplain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not includeinformation incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performancerequirements. For computer software it means data identifying source, functional characteristics,and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights" means the rights of the Government in limited rights data as set forth in theLimited Rights Notice of paragraph (g) (3) if included in this clause.

"Limited rights data" means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

"Restricted computer software" means computer software developed at private expense and thatis a trade secret, is commercial or financial and confidential or privileged, or is copyrighted computer software, including minor modifications of the computer software.

"Restricted rights," as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in thisclause, or as otherwise may be provided in a collateral agreement incorporated in and made partof this contract, including minor modifications of such computer software.

"Technical data" means recorded information (regardless of the form or method of the recording)of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computerdatabases (See 41 U.S.C. 116).

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, inany manner and for any purpose, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in—

(i) Data first produced in the performance of this contract;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance

and repair of items, components, or processes delivered or furnished for use under this contract;and

(iv) All other data delivered under this contract unless provided otherwise for limited rights dataor restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to—

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specificallyused by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data orrestricted computer software to the extent provided in paragraph (g) of this clause.

(c) Copyright—

(1) Data first produced in the performance of this contract.

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based onor containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data firstproduced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and an acknowledgment of Government sponsorship(including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by oron behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, withoutthe prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor—

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forthin paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyrightnotices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication, and use of data.* The Contractor shall have the right to use, release toothers, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except—

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance withsuch markings unless specifically authorized otherwise in writing by the Contracting Officer.

(e) Unauthorized marking of data.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, ifany data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g) (4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 4703, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety ofthe markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by theContracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject toany disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the headof the contracting activity, that the markings are not authorized, the Contracting Officer will

furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e) (1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the

Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modifiedin accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of thematter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) ofthe clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) Omitted or incorrect markings.

(1) Data delivered to the Government without any restrictive markings shall be deemed to havebeen furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized noticesplaced on the data at the Contractor's expense. The Contracting Officer may agree to do so if theContractor—

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproductionof any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may—

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the dataand demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(g) Protection of limited rights data and restricted computer software.

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause.As a condition to this withholding, the Contractor shall—

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Governmentshall be treated as limited rights data and not restricted computer software.

(h) *Subcontracting.* The Contractor shall obtain from its Subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a

Subcontractor refuses to accept terms affording the Government those rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or otherright otherwise granted to the Government.

(End of clause)

FAR 52.227-14 Addendum- Private Use of Data First Produced
The Contractor may not make use of any data first produced in the performance of the task order without the permission of the Contracting Officer as provided in FAR 52.227-14 paragraph (d)(2).

(End of clause)

FAR 52.244-6 Subcontracts for Commercial Products and Commercial Services (Sep 2023)

(a) Definitions. As used in this clause—

Commercial product, commercial service and *commercially available off-the-shelfitem* have the meanings contained in Federal Acquisition Regulation (FAR) 2.101.

Subcontract includes a transfer of commercial products or commercial services betweendivisions, subsidiaries, or affiliates of the Contractor or subcontractor at any tier.

(b) To the maximum extent practicable, the Contractor shall incorporate, and require its subcontractors at all tiers to incorporate, commercial products, commercial services, or non-developmental items as components of items to be supplied under this contract.

(c)

(1) The Contractor shall insert the following clauses in subcontracts forcommercial products or commercial services:

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (NOV 2021) (41 U.S.C. 3509), if the subcontract exceeds the threshold specified in FAR 3.1004(a) on the date of subcontract award, and has a performance period of more than 120 days. In altering this clause to identify the appropriate parties, all disclosures of violation of the civil False ClaimsAct or of Federal criminal law shall be directed to the agency Office of the Inspector General, with a copy to the Contracting Officer.

(ii) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5), if the subcontract isfunded under the Recovery Act.

(iii) 52.203-19, Prohibition on Requiring Certain Internal ConfidentialityAgreements or Statements (JAN 2017).

(iv) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (NOV 2021) , other than subcontracts for commerciallyavailable off-the-shelf items, if flow down

is required in accordance with paragraph (c) of FAR clause 52.204-21.

(v) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (NOV 2021) (Section 1634of Pub. L. 115-91).

(vi) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (NOV 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

(vii) 52.219-8, Utilization of Small Business Concerns (Sep 2022) (15 U.S.C.637(d)(2) and (3)), if the subcontract offers further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds theapplicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontractingopportunities.

(viii) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(ix) 52.222-26, Equal Opportunity (*Sept* 2016) (E.O.11246).

(x) 52.222-35, Equal Opportunity for Veterans (JUN 2020) (38 U.S.C.4212(a));

(xi) 52.222-36, Equal Opportunity for Workers with Disabilities (JUN2020)(29 U.S.C.793).

(xii) 52.222-37, Employment Reports on Veterans (JUN 2020) (38 U.S.C.4212).

(xiii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496), if flow down is required in accordance with paragraph (f) of FAR clause 52.222-40.

(xiv)

(A) 52.222-50, Combating Trafficking in Persons (NOV 2021) (22 U.S.C. chapter 78 and E.O.13627).

(B) Alternate I (MAR 2015) of 52.222-50(22 U.S.C. chapter 78 and E.O. 13627).

(xv) 52.222-55, Minimum Wages for Contractor Workers under Executive Order14026 (JAN 2022), if flow down is required in accordance with paragraph (k) of FAR clause 52.222-55.

(xvi) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2022) (E.O.13706), if flow down is required in accordance with paragraph (m) of FAR clause 52.222-62.

(xvii)

(A) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a) if flow down is required inaccordance with 52.224-3(f).

(B) Alternate I (JAN 2017) of 52.224-3, if flow down is required in accordancewith 52.224-3(f) and the agency specifies that only its agency-provided training is acceptable).

(xviii) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense AuthorizationAct for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

(xix) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (NOV 2021) , if flow down is required in accordance with paragraph (c) of FARclause 52.232-40.

(xx) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (NOV 2021) (46 U.S.C. 55305 and 10 U.S.C.2631), if flow down is required inaccordance with paragraph (d) of FAR clause 52.247-64).

(2) While not required, the Contractor may flow down to subcontracts for commercial products or commercial services a minimal number of additional clauses necessaryto satisfy its contractual obligations.

(d) The Contractor shall include the terms of this clause, including this paragraph (d), in subcontracts awarded under this contract.

(End of clause)

FAR 52.252-6 Authorized Deviations in Clauses (NOV 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)"after the date of the clause.

(b) The use in this solicitation or contract of any *Homeland Security Acquisition Regulation*(48 CFR *Chapter 30*) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

U. S. Department of Homeland Security Acquisition Regulation (HSAR) Clauses Incorporated by Full Text

The full text of the **Homeland Security Acquisition Regulation (HSAR)** may be accessed electronically at: http://www.dhs.gov/xlibrary/assets/opnbiz/hsar.pdf. All Homeland Security

Acquisition Regulation Clauses Incorporated in Full Text in the HCaTS basic IDIQ contract remain unchanged and in full force and effect. In addition, the HSAR Clauses listed in the sections below are hereby incorporated in Full Text to this RFP.

HSAR 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.

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

(h) 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.

(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)

HSAR 3052.205-70 Advertisements, Publicizing Awards, and Releases (Sep 2012)Alternate I (Sep 2012)

The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed
or preferred by the Federal Government or is considered by the Government to be superior toother products or services.

All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall theContractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

(End of clause)

HSAR 3052.242-72 Contracting Officer's Technical Representative (DEC 2003)

The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction,not less than five working days prior to giving the

contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.

The Contracting Officer cannot authorize the COTR or any other representative to signdocuments, such as contracts, contract modifications, etc., that require the signature of theContracting Officer.

The COR for this requirement is: [redacted]

(End of clause)

HSAR 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)

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)

HSAR Class Deviation 15-01, Revision 1 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)