SECTION I – SUPPLIES OR SERVICES AND PRICE/COSTS

1.0 TASK ORDER TYPE

This is a Labor-Hour task order under the Program Management, Administrative, Operations (Clerical), and Technical Services II (PACTS II), Functional Category 1 to provide Analyst Support Services in performing its mission to assist the Office for Civil Rights and Civil Liberties (CRCL) of the Department of Homeland Security (DHS).

2.0 TRAVEL

Contractor travel is not expected to support this requirement.

Costs for local travel and commuting expenses are not allowable; therefore, they will not be reimbursed for this task order.

3.0 SCHEDULE B

Contract Line Item Number (CLIN) 0001 **Base Period of Performance: 09/30/2022 – 09/29/2023**				
Government Labor Category	**Contractor Labor Category Title**	**Rate**	**Labor Hours**	**Extended Total**
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	

Program Manager	Senior Manager		200	

Contract Line Item Number (CLIN) 1001 **Base Period of Performance: 09/30/2023 – 09/29/2024**				
Government Labor Category	**Contractor Labor Category Title**	**Rate**	**Labor Hours**	**Extended Total**
Analyst (Intermediate) -	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Program Manager	Senior Manager		200	

Contract Line Item Number (CLIN) 2001 **Base Period of Performance: 09/30/2024 – 09/29/2025**				
Government Labor Category	**Contractor Labor Category Title**	**Rate**	**Labor Hours**	**Extended Total**
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	

Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Analyst (Intermediate)	Analyst4		1920	
Program Manager	Senior Manager		200	

Note: Hours between labor categories may be adjusted upon the Contracting Officer (CO) and Contracting Officer's Representative (COR) written approval as long as the obligated funding and task order ceiling are not exceeded. The contractor exceeds the obligated funding and task order ceiling at its own risk. The contractor shall notify the CO, Contract Specialist (CS), and COR in writing upon reaching 85% of the obligated funding and task order ceiling.

SECTION II - STATEMENT OF WORK

1 BACKGROUND

The U.S. Department of Homeland Security (DHS), Office of the Secretary, Office for Civil Rights and Civil Liberties (CRCL) supports the Department's mission to secure the nation while preserving individual liberty, fairness, and equality under the law. CRCL integrates civil rights and civil liberties into all of the Department activities by promoting respect for civil rights and civil liberties in policy creation and implementation by advising Department leadership and personnel, and state and local partners; communicating with individuals and communities whose civil rights and civil liberties may be affected by Department activities, informing them about policies and avenues of redress, and promoting appropriate attention within the Department to their experiences and concerns; investigating and making recommendations related to civil rights and civil liberties complaints filed by the public regarding Department policies or activities, or actions taken by Department personnel; and leading the Department's equal employment opportunity programs and promoting workforce diversity and merit system principles.

2 SCOPE

The purpose of this task order is to obtain Analyst Support Services to assist CRCL in performing its mission. The contractors shall perform analytical and administrative work in support of programs, the purpose of which is to evaluate and improve the efficiency, effectiveness,and productivity of CRCL's Branches and Sections.

3 REQUIREMENTS/TASKS

The contractor shall work in a high-volume production environment and perform a variety of duties necessary to ensure that CRCL's activities are conducted efficiently and effectively. There will be multiple positions with related but distinguishable tasks in one or more of the areas described below.

3.1 Compliance Branch Support

The contractor shall provide one (1) Intermediate Analyst to fulfill the following requirements:

The contractor shall work in a fast-paced environment and perform a variety of duties supporting the CRCL complaint process, civil rights and civil liberties investigations, and related projects.

Project management: The contractor shall have strong project management skills to plan and oversee projects or lead working groups to ensure that work is completed in a timely fashion and assigned goals are accomplished. This work shall include developing a project timeline, identifying necessary resources, monitoring progress, performing work on the project, and keeping stakeholders informed the entire way. (25%)

Process improvement: The contractor shall be able to understand business processes, analyze and evaluate them, propose changes, improvements, or best practices, and develop and implement plans for changes, training, and oversight of DHS business process improvements and modernization. (20%)

Support of the complaint process: The contractor shall be fully proficient with database technology to assist

with verification of data, running reports, and creating and analyzing performance metrics. The contractor shall be able to collect and organize materials, develop and maintain a library of relevant resources, and assist colleagues in finding information. (20%)

Support of investigations: The contractor shall be able to quickly review documents, identify and evaluate issues related to civil rights or civil liberties, and perform work in support of investigation of complaints related to these issues, and prepare oral or written work product as directed. This work is done under the guidance and direction of investigative staff. (25%)

Other projects and duties as assigned. (10%)

3.2 Anti- Discrimination Group Support

The contractor shall provide three (3) Intermediate Analysts to fulfill the following requirements:

The contractor shall provide technical and analytical support for the Civil Rights Evaluation Tool Program. The contractor shall review civil rights data, policies, and procedures under the direction of federal employees to determine whether they meet departmental requirements; provide detailed written and oral feedback to DHS grant recipients to ensure compliance with these requirements; and respond to grantee questions regarding compliance insufficiencies. The contractor shall identify and defines gaps and recommends methodologies and resources to develop and implement solutions related to compliance. The contractor shall produce frequent reports with key data (e.g., number of submissions; number of incomplete submissions; backlog rates); and evaluates trends from the data, including business processes. (50%)

The contractor shall organize and support virtual webinars and meetings; manage RSVP lists; and send out, compile, and evaluate information from webinar evaluations. The contractor must use accessibility checker for Power Point and other documents; and have experience or be willing to learn necessary steps for ensuring the accessibility of documents for compliance under Section 508 (40 %)

The contractors shall conduct basic research related to civil rights and/or grants management using public or governmental websites (USA Spending, OMB Max) to obtain information such as grant awards and civil rights compliance activities (10%)

3.3 Diversity Management Section

The contractor shall provide one (1) Intermediate Analysts to fulfill the following requirements:

The contractor shall work in a high-volume production environment and perform a variety of duties necessary to ensure that CRCL's activities are conducted efficiently and effectively.

The contractor shall assist the CRCL Statistician with the review of workforce demographic data for accuracy, and conduct workforce trend analysis as needed in support of EEO and Diversity programs. (25%)

In support of the EEOD strategic planning efforts, research and develop workforce, complaint, and reasonable accommodation data static dashboard visualizations; the contractor shall identify metrics for a

comprehensive EEO and Diversity dashboard that will include but not be limited to additional program areas to include Alternative Dispute Resolution and Anti-Harassment data. (25%)

The contractor shall create and develop an electronic database directory of minority serving institutions to support special emphasis program outreach efforts. This effort will be conducted in a phased approach, beginning with the creation of a HBCU directory. Phase two, will require the research and validation of the remaining Minority Serving Institutions (MSI). This task will also require the contractor to participate in strategic planning meetings, and implementation of quality control measures to ensure the continued success of the MSI database. (25%)

The contractor shall support and assist program managers with preparing annual EEO and diversity related reporting requirements. (10%)

The contractor shall develop diversity management related program materials, to include but not limited to web content, factsheets, brochures, and presentation materials. (15%)

3.4 Case Management Pilot Program - Data and Evaluation Support
The contractor shall provide one (1) Intermediate Analysts to fulfill the following requirements:

The contractor shall assist federal staff to develop CMPP program evaluation metrics, collect, and analyze CMPP data, and synthesize methodological and statistical analysis. Under the oversight of federal staff, the contractor will identify gaps and recommend methodologies and resources to develop and implement solutions related to CMPP evaluation and reporting

The contractor shall support CMPP program evaluation by working with federal staff and the CMPP Board to identify necessary datasets, develop and implement data collection and information sharing processes, and reporting strategies. The contractor shall produce periodic reports with key data to evaluate data trends from the data as defined by federal CMPP staff members. (40 %)

The contractors shall conduct basic research as directed by federal CMPP staff to support the CMPP Program (to include the CMPP Board and the CMPP Program Coordinator) as needed. (10%)

The contractor assists CMPP staff to using database metric to evaluate, review, analyze, and make recommendations related to CMPP. This work will be based on metrics analysis and/or statistical analysis completed by the contractor and provided to federal staff for review and completion. (50%)

3.5 Case Management Pilot Program - Program Support Analyst
The contractor shall provide one (1) Intermediate Analysts to fulfill the following requirements:

The contractor shall assist federal staff to develop and review CMPP programs, policies, and procedures to determine whether they meet departmental requirements.

The contractor shall provide detailed written and oral feedback to DHS grant recipients to ensure compliance with these requirements; and respond to and troubleshoot grantee questions as needed. The contractor shall assist to identify gaps in program services and shall work with federal staff to recommend methodologies and resources to develop and implement solutions related to compliance (15%)

The contractor shall work with federal staff to organize and support virtual webinars and in-person and virtual meetings; maintain and organize program filing system and provide support for CMPP Board meetings and outreach events. (15%)

The contractor shall work with federal staff to develop and implement a quality assurance program for CMPP service providers and will provide oversight and technical assistance to CMPP service providers, as needed. (50%)

The contractor shall conduct basic research related to case management, support CMPP Board Members, and support the CMPP Program Coordinators as needed, (20%)

3.6 Immigration Section Support
The contractor shall provide one (1) Intermediate Analyst to fulfill the following requirements:

The contractor shall work in a fast-paced environment and perform a variety of duties supporting the CRCL Immigration Section on training and meeting preparation and logistics, individual case inquiries, international human rights inquiries and tracking violations of statutory confidentiality protections under 8 USC 1367.

Trainings and Meetings: The contractor shall be able to organize and support virtual webinars and meetings, develop PowerPoint presentations, manage RSVP lists, take notes and summarize points made thematically. (20%)

Individual Case inquiries: The contractor shall be able to independently review and analyze individual immigration cases sent to CRCL with a request for CRCL to intervene and elevate to a DHS component. The contractor shall be able to enter the pertinent case details into CRCL's Microsoft Dynamics software platform, summarize the case details and identify the aspects of the case that present compelling civil rights and civil liberties factors. (25%)

Human Rights Inquiries: The contractor will provide analytical and technical support on taskers to DHS components regarding, inter alia, human rights reports, U.S. responses to petitioners, letters to treaty bodies, and talking points for meetings with UN and other human rights officials and meeting regarding human rights matters. This support includes keeping track of deadlines, conducting follow-up communications, combining component responses, and conducting research. (30%)

Tracking Violations of Confidentiality Protections: The contractor shall provide technical and analytical support for the Section 1367 Database. The contractor shall be responsible for inputting incoming notifications of potential violations into the database, analyzing initial information from the notification and follow up with Component's Privacy offices for addition information and/or clarifications. The contractor shall track all open cases in SwimLane and update the CRCL database with any relevant information and identify and define gaps into the investigation of the violations and make recommendations as required. The contractor shall produce frequent reports with key data (e.g., number of violations; type of violations; location of violations); and evaluate trends from the data. (25%)

3.7 Business Operations Section Support:
The contractor shall provide one (1) Intermediate Analysts to fulfill the following requirements:

The contractor shall work in a high-volume production environment and perform a variety of duties necessary to ensure that CRCL's activities are conducted efficiently and effectively.

The contractor shall assist the CRCL Executive Secretariat with the processing of taskers, which will require access to and training on a Correspondence Analyst Task Tracker (CATT) system. This is a face-paced environment with multiple and competing priorities. 25%

The contractor shall support and assist program managers with a variety of tracking mechanisms by reviewing reports and updating information contained in excel spreadsheets. 25%

The contractor shall support and assist program managers with reviewing a variety of written materials for accuracy, and in some cases updating the content of those written materials (for example, continuity of operations and emergency preparedness plan, reports and presentations) 25%

The contractor shall assist program managers with a variety of day-to-day business operations functions that may include mail management, physical inventory of asset for annual auditing purposes, etc. 25%

4 PERSONNEL

The government reserves the right to review and approve resumes of contractor personnel on this contract.

4.1 Program Manager

The Contractor shall provide a Program Manager (PM) who shall ensure all aspects of the task order are being adhered to and serve as the main point of contact for CRCL for all issues, including supervisory/management of personnel, human resource management, performance management, and quality assurance/quality improvement management. The Program Manager is further designated as *Key* by the Government. The name of the Program Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Program Manager, shall be provided to the Government as part of the Contractor's proposal. During any absence of the Program Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this task order. Additionally, the Contractor shall not replace the Program Manager without prior written approval from the Contracting Officer.

4.2 Analyst Support Contractors: Experience and Minimum Qualifications

The contractor shall provide nine (9) Intermediate Analysts to fulfill the requirements of the Statement of Work.

4.2.1 Compliance Branch Support Analyst

Experience:

The resume of the Compliance Branch Support Analyst shall demonstrate progressive professional or para-professional experience. This experience is defined as administrative, technical, or other analytical work that demonstrates the ability to acquire the knowledge and skills needed to perform the duties of the position as outlined in the SOW. Such experience includes familiarity with DHS policies, procedures, and systems.

Minimum Qualifications:

- 10+ years in accomplishing aforementioned roles and responsibilities.
- Strong written and oral communication skills to initiate, develop, and/or share communication of critical information in a variety of formats.
- Demonstrated success as a highly organized self-starter, with attention to detail, multitasking various priorities under deadline, and experience in a team environment.
- Demonstrated willingness to undertake new projects and ability to learn new systems.
- Proficient in Microsoft Office, especially Word, Excel, Outlook and PowerPoint.

4.2.2 Anti-Discrimination Group Support Analyst

The contractor shall provide three (3) Intermediate Analysts to fulfill the following requirements

Experience:

Resumes of the Anti- Discrimination Group Support Analyst contractors shall demonstrate progressive experience in database technologies, civil rights; grants management; and or other compliance programs. This experience is defined as technical work that demonstrates the skills and abilities to perform the duties of the position as outlined in the SOW Sections. The contractor shall have extensive experience with database technology and is able to resolve a wide range of issues related to database management in creative as well as practical ways.

Such experience includes familiarity with DHS or other governmental or non-governmental policies, procedures, and systems. Includes experience in using data system; compiling and tracking data; producing reports; planning and executing all aspects of virtual or in person meetings; reviewing and analyzing civil rights data.

Minimum Qualifications:

- A minimum of 2 years in civil rights field, grant compliance, or similar professional field.
- Demonstrated analytic skills, preferably as applied in a legal, civil rights, or grant compliance context.
- Expert written and oral communication skills.
- Experience in professional communication, both oral and written, with external stakeholders on complex federal requirements.
- Success as a highly organized self-starter, with attention to detail, meeting deadlines, and experience in a team environment.
- Experience with database technology, and with producing reports and analyzing data.
- Experience in planning, organizing, and supporting virtual meetings.
- Proficient in Microsoft Office, especially Word, Excel, Outlook and PowerPoint.
- Familiarity with the accessibility requirements of Section 508 and/or willing and able to learn and

apply accessibility requirements.

- Demonstrated success as a highly organized self-starter, with attention to detail, multitasking various priorities under deadline, and a customer-service oriented work ethic.
- Skill in Microsoft Power Bi is helpful but not required.

4.2.3 Diversity Management Group Support Analyst

The contractor shall provide one (1) Intermediate Analysts to fulfill the requirements

Experience:

The resume of the Diversity Management Group analyst support contractor shall demonstrate administrative and analytical experience with increasing responsibility.

This experience is defined as analytical and technical work that demonstrates the ability to acquire the particular knowledge and skills needed to perform the duties of the position.

Such experience includes familiarity with DHS policies, procedures, and systems; compiling and tracking data; providing computer assistance; excellent technical writing skills, research and analysis.

Minimum Qualifications:

- Expert written, and oral communication skills.
- Candidate must possess problem solving and research skills.
- Ability to interpret and analyze workforce and related data for triggers and barriers.
- Proficient in Microsoft Office, especially Word, Excel, PowerPoint, and Access
- Demonstrated success as a highly organized self-starter, with attention to detail, multitasking various priorities under deadline, and a customer-service oriented work ethic.
- Minimum of 5+ years' experience in accomplishing roles and responsibilities.
- Background experience in Equal Employment Opportunity, Diversity, and Inclusion, and/or Human Capital is desirable.
- Bachelor's degree from an accredited institution of higher education.

4.2.4 Case Management Pilot Program – Data and Evaluation Analyst Support

The contractor shall provide one (1) Intermediate Analysts to fulfill the requirements

The resume of the Case Management Pilot Program data and evaluation analyst contractor shall demonstrate experience in at least two, but preferably all of the following subjects: experience in evaluation science, database technologies, statistical analysis . This experience is defined as technical work that demonstrates the skills and abilities to perform the duties of the position as outlined. Also required is experience in using data systems; compiling and tracking data; producing reports; and reviewing and analyzing government and grantee data. Familiarity with DHS or other governmental or non-governmental policies, procedures, systems, and data would be preferred.

Minimum Qualifications:

- Advanced degree in public policy, social science, statistics, and/or program evaluation and analysis.
- Minimum of 2 years (preferably 5) in program evaluation or similar professional field.
- Demonstrated substantive skills, preferably in social services, immigration policy, civil rights, or grant compliance.
- Expert written and oral communication skills.
- Experience in professional communication, both oral and written, with external stakeholders on complex federal requirements.
- Success as a highly organized self-starter, with attention to detail, meeting deadlines, and experience in a team environment.
- Experience with database technology, and with producing reports and analyzing data.
- Experience putting together evaluation reports and providing evidence-based support for the conclusions.
- Experience in planning, organizing, and supporting virtual and in-person meetings to explain and understand evaluation needs.
- Proficient in Microsoft Office, especially Word, Excel, Outlook and PowerPoint.
- Demonstrated success as a highly organized, self-starter, with attention to detail, multitasking various priorities under deadline, and a customer-service oriented work ethic.

4.2.5 Case Management Pilot Program – Program Support

The contractor shall provide one (1) Intermediate Analyst to fulfill the requirements

The resumes of the case management pilot program support analyst contractor shall demonstrate experience in social work or case management programs, civil rights; grants management; quality assurance program implementation; or other compliance programs. This experience is defined as technical work that demonstrates the skills and abilities to perform the duties of the position as outlined in the SOW Sections. Familiarity with DHS or other governmental or non-governmental policies, procedures, and systems in preferred.

Minimum Qualifications:

- Advanced degree in social work, public policy, program management, or related field preferable.
- A minimum of 2 years (preferably 5) in social work and/or case management (preferably immigration-related), civil rights, grant management, or similar professional field.
- Expert written and oral communication skills.
- Experience in professional communication, both oral and written, with external stakeholders on complex federal requirements.
- Success as a highly organized self-starter, with attention to detail, meeting deadlines, and experience in a team environment.
- Experience with case management database technology, and with producing reports and analyzing data.
- Experience in planning, organizing, and supporting virtual and in-person meetings.
- Proficient in Microsoft Office, especially Word, Excel, Outlook, and PowerPoint.
- Demonstrated success as a highly organized, self-starter, with attention to detail, multitasking various priorities under deadline, and a customer-service oriented work ethic.

- Experience in planning, organizing, and supporting virtual and in-person meetings to explain and understand evaluation needs.
- Proficient in Microsoft Office, especially Word, Excel, Outlook and PowerPoint.
- Demonstrated success as a highly organized, self-starter, with attention to detail, multitasking various priorities under deadline, and a customer-service oriented work ethic.

4.2.6 Immigration Section

The contractor shall provide one (1) Intermediate Analyst to fulfill the requirements

Experience:

Resumes of the Analyst shall demonstrate progressive professional or para-professional experience. This experience is defined as administrative, technical, or other analytical work that demonstrates the ability to acquire the knowledge and skills needed to perform the duties of the position as outlined in the SOW

Such experience includes familiarity with DHS policies, procedures, and systems.

Minimum Qualifications:

- A minimum of 2 years in civil rights, human rights, immigration or similar professional field.
- Demonstrated analytic skills, preferably as applied in a legal, or civil rights context.
- Expert written and oral communication skills.
- Experience in professional communication, both oral and written, on complex topics.
- Success as a highly organized self-starter, with attention to detail, meeting deadlines, and experience in a team environment.
- Experience with database technology, and with producing reports and analyzing data.
- Experience in planning, organizing, and supporting virtual meetings.
- Proficient in Microsoft Office, especially Word, Excel, Outlook and PowerPoint.

4.2.6 Business Operation Section

The contractor shall provide one (1) Intermediate Analyst to fulfill the requirements

Experience:

The resume of the Business Operations Support Analyst shall demonstrate progressive professional experience. This experience is defined as administrative, technical, or other analytical work that demonstrates the ability to acquire the knowledge and skills needed to perform the duties of the position as outlined in the SOW.

Such experience includes familiarity with DHS policies, procedures, and systems.

Minimum Qualifications:

- 10+ years in accomplishing aforementioned roles and responsibilities.
- Strong written and oral communication skills to initiate, develop, and/or share communication of critical information in a variety of formats.
- Demonstrated success as a highly organized self-starter, with attention to detail, multitasking various priorities under tight deadlines, and experience in a team environment.

- Demonstrated willingness to undertake new projects and ability to learn new systems.
- Proficient in Microsoft Office, especially Word, Excel, Outlook and PowerPoint.

4.3 KEY PERSONNEL

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced. The Contractor shall not replace *Key* Contractor personnel without acknowledgment from the Contracting Officer. The Program Manager, Analyst Support labor categories are key personnel under the award.

5.0 GENERAL REPORTING REQUIREMENTS

The contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS Microsoft Office applications.

5.1 PROGRESS REPORTS.

The Program Manager (Contractor) shall provide progress reports as needed to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including an assessment of technical progress, written and analytical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

5.2 PROGRESS MEETINGS.

The Contractor shall be available to meet with the COR or CRCL POC upon request to present deliverables, discuss progress, exchange information and resolve emergent problems and issues. These meetings shall take place at the Government's facility or via telephone or email.

6 INTELLECTUAL PROPERTY.

All reports generated, documentation produced, and research conducted in the performance of this requirement shall be the property of DHS.

7 PROTECTION OF INFORMATION.

Contractor access to information protected under the Privacy Act is required under this contract. Contractor access to unclassified Security Sensitive Information and Law Enforcement Sensitive information will be required under this contract. This documentation will be provided to the Contractor in person, by mail, or by email. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

The Contractor shall be required to submit a signed Non-Disclosure Agreement hereby incorporated as "Non-Disclosure Agreement."

8 GOVERNMENT FURNISHED RESOURCES.

Work will be performed at the Government's site. The Government will provide the Contractor with the following resources for all onsite Contractor personnel: to include enough workspace, computers, telephones, access to printers, access to photocopiers, and access to scanners.

The Government furnished facilities, property, equipment and supplies issued to the Contractor shall only be used for work under this task order. The Contractor shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear.

The Government will provide all necessary information, data and documents to the Contractor for work required under this task order.

The Government will provide a government furnished laptop and a government furnished mobile cell phone.

SECTION III – DELIVERIES AND PERFORMANCE

1.0 PERIOD OF PERFORMANCE

The period of performance for work performed under this contract consists of a one-year base period of performance, and two (2) one-year optional periods of performance.

2.0 PLACE OF PERFORMANCE

The primary place of performance shall be CRCL's office at 2701 Martin Luther King Jr. Ave, Washington, DC 20032.

3.0 HOURS OF OPERATION

The core hours of operation shall be between the hours of 8am and 5pm Monday through Friday, except on Federal holidays.

4.0 TRAVEL

Contractor travel is not expected to support this requirement.

5.0 GOVERNMENT HOLIDAYS

Holidays observed by the Federal Government:

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

If a holiday falls on Sunday, the following Monday will be observed as the legal holiday.

When a holiday falls on a Saturday, the preceding Friday is observed as a legal holiday by U.S.

Government agencies. Also included would be any day specifically declared by an Executive Order from President of the United States of America as a national holiday.

It is understood and agreed between the Government and the Contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement to compensation except as set forth within this task order. If the Contractors believes that an unplanned absence has an impact on the price or period of performance, it should notify the Contracting Officer.

6.0 TELEWORK

It is the policy of the Department to make telework available to the maximum extent possible without negatively impacting mission accomplishment. Participation in a telework arrangement is a management prerogative and not an employee/contractor entitlement or right. All CRCL contractor requests for telework must be submitted in writing by using the CRCL Telework Agreement and approved or disapproved in writing by the CRCL COR and the contractor PM.

Situational: Contractors who anticipate that they will occasionally request telework must complete and sign a Telework Agreement, which will be maintained on file by the Contracting Officers Representative (COR). Each time a contractor wishes to telework, he or she must seek approval from the COR, providing as much advance notice as possible. The COR and CRCL support Manager will consider office coverage and business needs prior to approving or denying the request.

Emergency. On very rare occasions, CRCL contractors may be required to telework due to unexpected events or disasters (e.g., COOP-related or non-weather-related building closure). Because these events cannot be anticipated, all CRCL contractors must sign a Contingency Telework Agreement to be effective in the case of an emergency situation.

Telework Requirement: The contractor shall log on, and remain logged on, to communication software throughout the entire workday as outlined by CRCL.

7.0 CONTRACTOR'S RESPONSIBILITY FOR ASSIGNED EQUIPMENT, AND SUPPLIES

If, due to the fault or neglect of the Contractor, his agents, or employees, damages are caused to any Government property, equipment, stock or supplies, during the performance of this contract, the Contractor shall be responsible for such loss or damage and the Government, at its option, may either require the Contractor to replace all property or to reimburse the Government for the full value of the lost or damaged property.

8.0 DELIVERABLES

The Government will review all draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance with government policies, regulations,

laws and directives. Written documents shall be concise and clearly written.

Final documentation deliverables shall be provided in hard and soft copy using MS Office applications. Daily, weekly and interim information deliverables and working-copy products may be provided by email, as arranged with the COR.

All deliverables shall be submitted to the COR and assigned CRCL POC identified in this contract. A copy of the bi-monthly Status/Activity Report shall be submitted to the COR and the Contracting Officer.

8.1 Bi-Monthly Status Meeting

The Contractor shall meet with the Contracting Officer's Representative (COR) on a bi-monthly basis to discuss progress under the SOW. The purpose of the status meeting is to exchange information and assist in the resolution of emergent technical problems and/or issues.

8.2 Project Plan

The Contractor shall provide a draft Project Plan at the Kick-off meeting. The final Project Plan shall be provided to the COR within 5 days of the draft Project Plan's approval. The Project Plan shall include:

- Start Up Phase
- Business Approach and
- Summary of deliverables.

8.3 Status/Activity Report

The status/activity report shall be submitted every two weeks beginning two weeks from task order award and shall include at a minimum the following:

a) Financial Summary of labor hours funded , projected spending, funds remaining, and actual invoices per Contract Line item
b) Summary of Contract Information
c) Summary of tasks completed by contractors during the period of the report .
d) Total Labor hours worked for each contractor during the reporting period A

8.4 Daily Assignment Logs from Contractors

The daily assignment logs from the contractors shall include:

- Daily log-on email noting the date and time the contractor logs on to start work.
- Daily log-off email listing the time blocks and brief description of task performed in hourly intervals.

Or any updates as requested by the COR.

8.5 Monthly Leave Calendar for contractors

The monthly leave calendar shall include the names of the contractors and anticipated days for time off within the period of reporting. The contractor shall inform the COR and CRCL POCs by email of upcoming leave and changes to schedules, including early/unanticipated log off.

DELIVERABLES AND DELIVERY SCHEDULE

Item	Reference	Event/Deliverable	Date Due	Format	Distribution
1	Section IV.1	Post Award Conference	Within Five (5) Business Days of Task Order Award or as coordinated by CO/CS	In person meeting or Via Teleconference	CO/CS and COR
2	Section 1V.2	Kick Off Meeting	Within seven (7) Business Days of Task Order Award or as coordinated by the COR	In person meeting or Via Teleconference	COR
3	Section III 8.2	Draft Project Plan	Concurrent with the Kick-Off Meeting	MS Office	CO/CS and COR
4	Section III 8.2	Final Project Plan	Within 5 days of the draft Project Plan Approval	MS Office	CO/CS and COR
5	Section II 5.1	Progress Report	As requested by the CO and COR	MS Office	CO/CS and COR
6	Section II 5.2	Progress Meeting	Bi-Monthly	In Person or via Teleconference	COR
7	Section III 8.3	Status/Activity Report	Bi-Weekly	MS Office	CO/COR

8	Section III 8.4	Daily Work Assignment Logs from Contractors	Daily	Electronic	COR/CRCL POC
9	Section III 8.5	Calendar Leave Log	Monthly, First week of the month	Electronic	COR/CRCL POC

9.0 508 Compliance

Section ADA 508C refers to Section ADA 508C of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). Section ADA 508C assessments are required of all systems and are intended to ensure that individuals with disabilities have comparable access to and use of information and data comparable to the access provided to individuals without disabilities (unless this would pose an undo burden on the Federal Agency). The assessment is not to include physical access at any defined-benefit technology solution-related site. The ADA 508C assessment shall be performed by OPM. The successful Contractor must make accessible to the Government, or its designee, information systems residing in the Contractor's (or as appropriate sub-Contractor's) facilities that support the operations and assets of the Government as part of this task order, so that the ADA 508C assessment may be performed.

All Electronic and Information Technology (EIT) procured through this task order must meet the applicable accessibility standards at 29 USC 794d and 36 CFR 1194, unless an exception to this requirement exists as determined by the Government. See 29 USC 794d at http://www.section508.gov/index.cfm?Fuseaction=Content&ID=12, and 36 CFR 1194 implementation Section ADA 508C of the Rehabilitation Act of 1973, as amended, at http://www.access-board.gov/secADA 508C/ADA 508C standards.htm - PART 1194 .

The following standards are applicable to this procurement:

1. 1194.21 Software applications and operating systems.
2. 1194.22 Web-based intranet and Internet information and applications.
3. 1194.23 Telecommunications products.
4. 1194.24 Video and multimedia products.
5. 1194.31 Functional performance criteria.
6. 1194.41 Information, documentation and support.

NOTE: The ADA 508C standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

SECTION IV – CONTRACT ADMINISTRATION DATA

1.0 POST AWARD MEETING

The Contractor shall participate in a Post Award Meeting with the Contracting Officer and the COR no later than five (5) business days after the date of award. The purpose of the Post Award Meeting is to discuss the contracting objectives of this contract. The Post Award Meeting will be held at the Government's facility or via teleconference or conference call.

2.0 KICK-OFF MEETING

The Contractor shall attend a Kick-Off meeting with the COR and members of the Program Office no later than 5 business days after the date of award. The purpose of the Kick-Off meeting, which will be chaired by the COR, is to discuss the technical objectives of this contract. The Kick-Off meeting will be held at the Government's facility, located in Washington, DC or via teleconference or conference call. The specifics of the meeting will be provided upon contract award.

3.0 CONTRACTING OFFICER

The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds and authorize revisions of the terms and conditions of this contract. The Contracting Officer shall authorize any such revision in writing.

The Contracting Officer is:

Note: The Contracting Officer's contact information is

4.0 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The Contracting Officer will designate in writing a Contracting Officer's Representative (COR) to assist in monitoring the work under this contract. The COR is responsible for the technical administration of the contract and technical liaison with the Contractor. The COR is not authorized to change the scope of work or specifications as stated in the contract, to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract price, delivery schedule, period of performance, or other terms or conditions. The Contractor will receive a copy of the COR Appointment Letter outlining the roles and responsibilities of the COR.

The COR for this contract is:

Note: The COR's contact information is

SECTION V - INVOICE AND PAYMENT PROVISIONS

1.0 INVOICES

Invoices shall be prepared in accordance with FAR Clauses 52.232-7 Payments under Time-and-Materials and Labor-Hour Contracts. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

a) Cover sheet identifying DHS;
b) Contract Number;
c) Modification Number, if any;
d) DUNS Number; ??
e) Month services provided
f) CLIN and Accounting Classifications

The Contractor shall submit one invoice by the 5th day of each month.

Contract Line Item Number (CLIN) for each billed item:

a) Time and Materials and Labor Hour – Invoices shall be submitted no more than once per month and shall be received no later than the 5th of each month (or as otherwise approved by the COR) following the services provided. The Contractor shall indicate the associated CLIN, dollar amount invoiced, and service completed. All invoices shall include the current amount billed along with a cumulative amount billed and remaining balance.

The Contractor shall submit the invoice electronically to the address below:

E-mail: InvoiceMGT.Consolidation@ice.dhs.gov

The Contractor shall simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

a) ATTN: (Contracting Officer)

E-mail:

c) ATTN: on (COR)

E-mail:

SECTION VI – SPECIAL CONTRACT REQUIREMENTS

1.0 CONTRACTOR PERSONNEL SECURITY CLEARANCE REQUIREMENT

All contractor and subcontractor personnel are required to complete a suitability/background investigation with the DHS Office of Security, Personnel Security Division.

The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process suitability/background investigations and suitability determinations, as required, in a timely and efficient manner.

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

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

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

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

DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a

favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and nonrecurring meetings in order to begin transition work.

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

When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated suitability/background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

2.0 SECURITY OFFICE CONTACT

Office of Security/PSD

Customer Service Support

Washington, DC 20528

Telephone: [redacted]

E-mailbox: [redacted]

3.0 NON-DISCLOSURE AGREEMENT

The Contractor shall submit an executed Non-Disclosure Agreement (Attachment I) for each individual performing under this contract. The Contractor shall submit copies of the Non-Disclosure Agreement to the Contracting Officer and COR prior to an individual beginning performance under this contract.

4.0 DISCLOSURE OF INFORMATION

Information furnished under this contract may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personnel information must be clearly marked. Marking of items will not

necessarily preclude disclosure when DHS or the Government determines disclosure is warranted by FOIA. However, if such items are not marked, all information contained within the submitted documents will be deemed to be releasable.

Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the provisions of this contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.

In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees.

Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 USC 641.

5.0 DISCLOSURE OF INFORMATION LITIGATION

Contractor employees shall comply with 6 C.F.R. Part 5, Subpart C, including 6 C.F.R. §§ 5.44 and 5.49. Those regulations generally prohibit contractor employees from testifying in connection with litigation based upon information acquired in the scope and performance of their official Department duties, except as authorized by the Department.

6.0 NON-PERSONAL SERVICES

The services required under the contract constitute professional support services, which are essential to the mission but not otherwise available within. The Government will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual Contractor employees. It shall be the responsibility of the Contractor to manage their employees and to guard against any actions that have the nature of personal services or give the perception of personal services. If the Contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's further responsibility to notify the Contracting Officer immediately.

These services shall not be used to perform work of a policy/decision making or management nature. All decisions relative to programs supported by the Contractor will be the sole responsibility of the Government. Support services will not be ordered to circumvent personnel ceilings, pay limitations, or competitive employment procedures.

7.0 EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities 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.

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.) and display the Government-issued badge in plain view above the waist at all times.

8.0 EMPLOYEE CONDUCT

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

9.0 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion, 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.

10.0 OTHER APPLICABLE CONDITIONS

10.1 Security

Contractor access to unclassified, but Sensitive Security Information (SSI) or Personally Identifiable Information (PII), may be required under this contract. Contractor staff members shall safeguard this information against unauthorized disclosure or dissemination. Contractor staff members are not required to have a security clearance; however, a background investigation and a suitability determination will be conducted on contractor personnel assigned to this contract.

10.1.1 Protection of Information

Contractor access to sensitive but unclassified information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to

business or procurement-sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

10.1.2 Contractor Employee Access

Sensitive Information, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

a) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
b) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal
c) Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," 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 his/her designee);
d) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and,
e) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

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 sensitive information or IT 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. 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.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

a) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.
b) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.
c) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).
d) 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.

- 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:
    - The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
    - There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
    - The waiver must be in the best interest of the Government.

e) 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.

10.1.3 Personal Identification Verification (PIV) Credential Compliance

Authorities:

- HSPD-12 "Policies for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-06-16 "Acquisition of Products and Services for Implementation of HSPD-12"
- NIST FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- NIST SP 800-63 "Electronic Authentication Guideline"
- OMB M-10-15 "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(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.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. 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 also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the 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.

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of

PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," 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 his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)

(2) Date of birth (month, day, and year)

(3) Citizenship or immigration status

(4) Ethnic or religious affiliation

(5) Sexual orientation

(6) Criminal History

(7) Medical Information

(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification,

upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or

Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, 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) Data Universal Numbering System (DUNS);
(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, email);
(v) Contracting Officer POC (address, telephone, 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 sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy 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 sensitive information 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, and
(iv) Data analyses and processing.

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

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions 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 and 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, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information 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; and/or

(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 FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

SECTION VII – TASK ORDER CLAUSES

1.0 INCORPORATED BY REFERENCE

The Contractor's OASIS contract clauses are incorporated into this task order. This document also includes one or more clauses by reference with the same force and effect as if they were given in full text in accordance with the Federal Acquisition Regulation (FAR) Clause 52.252-2, "CLAUSES INCORPORATED BY REFERENCE." Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address: http://acquisition.gov/far/ or for DHS specific clauses at http://farsite.hill.af.mil/VFHSAR1.html

Clause	Title	Date
FAR Clauses Incorporated by Reference		
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	Apr 2014
52.222-50	Combating Trafficking in Persons	Mar 2015
52.224-1	Privacy Act Notification	Apr 1984
52.224-2	Privacy Act	Apr 1984
52.227-14	Rights in Data – General	Jun 1987
HSAR Clauses Incorporated by Reference		
30521.205-70	Advertisements, Publicizing Awards and Releases	Sept 2012
3052.242-72	Contracting Officer's Technical Representative	Dec 2003

2.0 INCORPORATED BY FULL TEXT

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 60 days of contract period expiration.

(End of clause).

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

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

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

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

(End of clause).

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

Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)

(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 in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by 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 with Kaspersky Lab; or

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

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any 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 or deliverables first produced in the performance of the contract.

(c) *Reporting requirement.*

(1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or 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 in the report provided at https://dibnet.dod.mil.

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

(i) Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a 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 of covered articles.

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

(End of clause)

FAR 52.204-25: PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT.

As prescribed in 4.2105(b), insert the following clause:

Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020)

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

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

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

Covered telecommunications equipment or services means–

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

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

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

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

Critical technology means–

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

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

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

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

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

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

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

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act 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 off traffic where it is ultimately delivered (*e.g.*, connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

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

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

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

(b) *Prohibition*.

(1) Section 889(a)(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 extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses

any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

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

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

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

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the 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 in the report provided at https://dibnet.dod.mil.

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

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

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

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

(End of clause)

HOMELAND SECURITY ACQUISITION REGULATION (HSAR) CLAUSES

HSAR 3052.215-70 Key Personnel or Facilities (Dec 2003)

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

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

The Key Personnel or Facilities under this Contract:

- **Program Manager**
- **Senior Office Clerk**
- **Office Clerk (all personnel)**

(End of Clause)

HSAR 3052.204-70 Security Requirements for Unclassified Information Technology Resources (Jun 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach

contained in the quoter's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

HSAR 3052.204-71 Contractor Employee Access – Alternative I (Sep 2012)

(a) *Sensitive Information,* as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been

specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

> (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
>
> (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," 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 his/her designee);
>
> (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
>
> (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(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 sensitive information or IT 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 sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

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

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

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

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. 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)

HOMELAND SECURITY ACQUISITION REGULATION (HSAR) PROVISIONS

HSAR 3052.209-70 Prohibition on Contracts with Corporate Expatriates (Jun 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) *Plan deemed in certain cases*. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain transfers disregarded*. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special rule for related partnerships*. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;

(ii) options;

(iii) contracts to acquire stock;

(iv) convertible debt instruments; and

(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) *Disclosure.* The offeror under this solicitation represents that [Check one]:

__ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of provision)