REVISED P00008 - ATTACHMENT I

U.S. Department of Homeland Security
Office of Strategy, Policy, and Plans
Center for Prevention Programs and Partnerships (CP3)

Statement Of Work
CP3 Strategic Communications Support

1 GENERAL

1.1 Introduction

The United States remains in a heightened threat environment from targeted violence and terrorism, and several recent attacks have highlighted the dynamic and complex nature of the threat. As the DHS lead for targeted violence and terrorism prevention, the Center for Prevention Programs and Partnerships ("CP3") helps communities prevent targeted violence and terrorism and build a safer America. To achieve that goal, CP3 develops partnerships across every level of government, the private sector, and in local communities across our country to provide funding, training, educational resources, and to increase awareness.

1.2 Background: Pivot to National-Level Focus

CP3 has a strong record of supporting communities in strengthening their capacity to prevent targeted violence and terrorism. Currently, CP3 is working to scale its prevention activities across the country, increase national awareness of its mission, and to rigorously evaluate its impact.

CP3's priorities include:

- Supporting state governments and their creation of targeted violence and terrorism prevention (TVTP) strategies.
- Identifying performance and outcome metrics that can form the basis for continual assessment and performance improvement.
- Examining how to engage stakeholders more routinely and how to continue to build trust.
- Promote sharing of information and promising practices in violence prevention among TVTP grantees and increase equity in the TVTP grant program.[1]
- Enhancing CP3 brand awareness among all relevant stakeholders as well as public awareness of CP3 products, resources, information, training, and events.

Broadly, the Contractor will augment CP3 activities by providing ad hoc support to grantmaking and logistics, prevention education material creation and delivery, collection and analysis of research, supporting strategic planning and information sharing among CP3 teams, media analysis, and administrative support as needed. The Contractor will also provide field operations analysis, including analysis of regional threats, analysis of regional community and stakeholder needs across the country, engagement strategies for communicating with new audiences, analysis of regional prevention stakeholders and programs, analysis of local media on targeted violence and terrorism, analytic support

[1] CP3 is also looking to strengthen the coordination between the TVTP grant program and more expansive preparedness grant programs managed by FEMA.

to support the development of state strategies, and assistance with logistics of regional events for leadership.

1.3 Key Deliverables and Objectives, by Priority Area

Contractor deliverables will revolve around supporting CP3's core functions, as articulated above. Key deliverables shall include:

- *Foundational Prevention Research*
  - Review existing bystander hesitancy research to develop lessons learned for the prevention of targeted violence and terrorism.
  - Testing to determine what messages motivate individuals to get help for people they are concerned about before harm occurs.
- *Support to State Strategy Development and Amplifying Best Practices*
  - Research on existing and promising state level prevention approaches as well as what existing frameworks states have in place. Provide recommendations on how to fill identified prevention gaps
- *Stakeholder Engagement*
  - A landscape analysis of other organizations operating in the prevention space (and existing prevention and deradicalization resources), to help CP3 identify existing evidence-based and promising practices and opportunities for partnership, note and avoid areas of overlap, and determine national prevention gaps that CP3 may fill.
- *Improving the TVTP Grant program and Strengthening Coordination with Other DHS Preparedness Grant Programs*
  - Support CP3 efforts to engage current and potential grantees, with a particular focus on increasing equity in DHS grant awards and elevating and replicating best practices.
- *Enhancing CP3 Brand Awareness and Public Awareness*
  - Periodically reviewing and updating CP3 products, resources, information, training, and events to ensure they remain digestible, accessible, empathetic, and intuitive and reflect relevant cultural sensitivities.
  - A long-term communications strategy, inclusive of social media, which identifies primary communication channels and mediums to reach audiences and enhance CP3's efforts to deliver resources to individuals and relevant organizations to help their communities prevent targeted violence and terrorism.
  - Developing and refining core messages and talking points for use with internal and external stakeholders, ensuring consistency across CP3 and alignment with current targeted violence and terrorism prevention research.

All developed and approved messaging and materials should leverage industry leading technical, audio, and visual media techniques and platforms to bolster the delivery and increase the adoption of messaging across all stakeholders. All messaging and materials should be highly accessible to the public, including by using plain language and avoiding jargon.

All final materials shall be provided to DHS and are subject to DHS written approval prior to public release.

2 SPECIFIC COMMUNICATIONS/BRAND AWARENESS REQUIREMENTS/TASKS

2.1 Task 1 – Communications Research, Analysis, and Planning

The contractor shall assist the Government with establishing plans, performance measures, reviews, and assessments related to developing and implementing communications strategies. The contractor shall work with stakeholders to produce schedule designs, project management plans, milestones, and metrics. The contractor shall incorporate recommendations and findings from new or existing research into the execution and implementation plans and communications strategies. The contractor shall provide collaboration and coordination support throughout the process of planning, implementing, producing, and post-engagement support. The contractor shall assist in researching information, including from various sources to support CP3 communications activities.

The contractor shall coordinate with analysts and senior managers through the planning cycle to ensure that documents are compliant with applicable standards, coordinated through leadership, and developed in a timely manner to the appropriate audience. Examples of such communications research, analysis, and planning activities include but are not limited to;

- Developing project management and strategic planning tools, such as project management plans, milestone tables, etc.
- Reviewing CP3 products, resources, information, training, and events to ensure they remain digestible, accessible, empathetic, and intuitive and reflect relevant cultural sensitivities.

2.2 Task 2 – Content Development and Delivery

The Contractor will help CP3 develop tailored content for members of the public as well as key prevention practitioners and stakeholders (including, but not limited to, faith-based organizations, civic and community organizations, educational institutions, etc.).

The contractor shall, upon request, perform the following:

a. Provide translation services for CP3 materials (print and digital). Required translation languages must include English, Spanish, French and Arabic. Additional languages may be requested based on product and demand, and as directed by the DHS Office for Civil Rights and Civil Liberties. Translators must be native speakers to ensure translations are culturally and grammatically aligned with the respective language. Translations should have dual party reviews to ensure accuracy. A second party (not the translator) should review the product prior to submitting to DHS. Material should be developed in "plain/common language" and should be easily understood by the general public.

b. Provide all ancillary personnel required for the development of, but not limited to, print work, public service announcements, speaking engagements and/or training videos (i.e., actors, spokespersons, etc.).

c. Develop alternate versions of existing creative and products based on divergent stakeholder requirements, perform other modifications to existing creative and products upon request, and incorporate previous versioning into new and existing products and materials.

d. Revise and update existing creative and products based on evolving requirements. Provide direct

support for the writing and editing of materials, which may include video, radio, television, public service announcements, talking points, briefing memos, pamphlets, brochures, leaflets, and web pages/sites.

e. Support the development and implementation of routine and ad hoc communication activities that meet objectives outlined in CP3 communications strategy to include, but not limited to:
   - Quarterly Newsletter
   - Regional Prevention Success Stories
   - TVTP Grant Success Highlights
   - CP3 Annual Report
   - Monthly Blog Posts
   - Social Media Content
   - Press Releases
   - Talking Points
   - Briefing Memos

f. Support the design, development, and implementation of national campaigns to reach bespoke audiences and empower communities with tailored prevention information.

g. Ship and print materials or other tools and resources to stakeholders via an international carrier (FedEx, UPS, etc.). Vendor will provide shipping capability, and all associated costs will be reimbursed.

To facilitate content delivery, the Contractor shall provide technical and advisory services to assist DHS in its publication and delivery of prevention resources. The Contractor will advise on how best to technically integrate content into existing channels, such as websites, social media, mobile applications, and other digital means. The contractor shall conduct an analysis of current communication channels, identify new channels and develop metrics to track effectiveness of channels to determine which should be kept and which removed, to more efficiently communicate with all stakeholders and partners.

Examples of such content delivery activities include but are not limited to:

- Stand up national, regional, and/or local focus groups and listening sessions, including in underserved and/or rural communities, to test CP3 messaging and provide a report with findings and recommendations to CP3 leadership ~~that reflect appropriate diversity, inclusion and equity of participants and the general public~~.
- Incorporate inventory codes and other versioning into new and existing creative products.

The contractor shall develop standard operating procedures for all new communication channels and metrics to monitor implementation and success of communication delivery. Finally, the Contractor will ensure that all products, services, and personnel are compliant and adhere to civil rights and civil liberties and privacy protections ~~and reflect diversity, inclusion and equity principles~~ provided from the Program Manager and COR.

2.3 Task 3 – Professional Events and Nationwide Support

The contractor shall support DHS in the planning, execution, and success measurement of CP3 events. Events include, but are not limited to, themed forums, panels, roundtables, listening sessions, and conferences. Such support may include securing venues, designing collateral, managing vendors, providing on-site support, and securing speakers and attendees as required. The contractor shall also support CP3 by securing speakers at costs not to exceed limits as set forth by DHS. These limits do not include travel or per diem costs as those costs are determined by GSA and governed by the Joint Travel Regulations.

2.4 Task 4 – Order Level Materials

The Government will provide a Not to Exceed (NTE) Order Level Materials (OLM) CLIN to support products and services not explicitly named and priced within Attachment II, Pricing Schedule.

Examples of Order-Level Materials related to this Task Order include, but are not limited to:

- Video and Audio Production – Filming/recording in studios, on location, live shows, etc. (to include writing, directing, shooting, arranging for talent/animation, narration, music and sound effects, duplication, distribution, video scoring, editing, post production, final delivery)
- Photography (to include photo shoots, unique shots, delivery of finished shots, etc.)
- Custom Illustration - Planning, designing, and managing the production of visual communication in order to convey specific messages or concepts, clarify complex information, or project visual identities
- Exhibit Design and Implementation - Conceptualizing, designing and producing exhibits and their accompanying materials

3 Task Order Deliverables

Deliverable	Due Date	Recipient	Format
Foundational Prevention Research Report with findings, analysis, and recommendations	March 31, 2023	COR & CP3 Program Manager	Electronic format (e.g., Microsoft Word, Adobe Portable Document Format)
Stakeholder Landscape Analysis, including promising state level approaches, and recommendations on how to fill identified prevention gaps	May 31, 2023	COR & CP3 Program Manager	Electronic format (e.g., Microsoft Word, Adobe Portable Document Format)
Communication Strategy, to include stakeholder engagement plans informed by research, and success metrics	NLT than 12 weeks after research findings approved by DHS.	COR & CP3 Program Manager	Strategy will be delivered in a mutually agreed upon format.

Content Development and Delivery	Ongoing task	COR & CP3 Program Manager	Will be delivered in a mutually agreed upon format depending on content type - in alignment with
TVTP Grantee Engagement Plan	February 28,	COR & CP3 Program Manager	Electronic format (e.g., Microsoft Word, Adobe Portable Document Format)
Project Management and Strategic Progress Reports, including weekly updates and monthly progress summaries produced on behalf of executive leadership.	Ongoing task	COR & CP3 Program Manager	Electronic format in project management software and PDF file
Periodic reviews of CP3 products, resources, information, training, and events to ensure they remain digestible, accessible, empathetic, and intuitive and reflect relevant cultural sensitivities.	Ongoing task	COR & CP3 Program Manager	Electronic format in project management software and PDF file

4. OTHER WORK MATTERS

4.1 Place of Performance

The Contractor will generally perform the work under this contract at the Contractor's Facility. The Contractor may be required to perform services, including in person meetings, at the DHS St. Elizabeth's Campus located in Southeast Washington, DC. Parking facilities are not provided at Federal Government Facilities. As required, the place of performance may be other than the Contractors facility, and in such instances, it shall be mutually established by the Contractor and the Contracting Officer and Contracting Officer Representative based on in-scope tasks being performed and deliverables being prepared.

4.2 Period of Performance

The total period of performance for this Task Order is three (3) years consisting of the following:

Base Period: 12 months
Option Period 1: 12 months
Option Period 2: 12 months

4.3 Progress Meetings

The Project Manager shall be available to meet with the COR and Federal Program Manager upon request to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place in person at the Government or Contractor's facility.

4.4 Continuity of Support

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

5 TASK ORDER PERSONNEL

The contractor shall be responsible for employing technically qualified personnel to perform the work specified in this statement of work. The contractor shall maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the government's specifications and requirements. The work history of each contractor employee must contain experience directly related to work he/she is required to perform under this Task Order.

5.1 Contractor Project Manager

The contractor shall provide a dedicated Project Manager who shall be responsible for all contractor work performed under this Task Order. The Project Manager is further designated as Key by the government.

The Project Manager shall be a single point of contact for the Contracting Officer (CO) and the Contracting Officer's Representative (COR). It is anticipated that the Project Manager shall be one of the senior level employees provided by the contractor for this work effort. The Project Manager and all designated alternates shall be able to fluently read, write, speak, and understand English.

The Project Manager shall be available to the Federal Program Manager and COR via telephone or e-mail five days a week between the hours of 9:00 AM and 5:00 PM ET and shall respond to a request for discussion or resolution of technical problems within one hour of notification. If the Project Manager is scheduled to be out of the office, DHS requests at least three (3) days' notice and a designated point of contact during the PM's absence.

The Project Manager is responsible developing and managing project plans and schedules based on assigned tasks as well as conducting weekly status updates meetings with the Government. The contractor is responsible for capturing and reporting notes from all meetings. Meeting notes will be provided to the COR and Program Manager within forty-eight hours (48) of the meeting.

5.2 Contractor Key Personnel

The Contractor shall propose a staffing plan that identifies Key personnel. The Contractor's Project Manager is designated as Key Personnel. The Contractor must provide documentation (e.g., a resume)

detailing the Project Manager possesses experience detailed in the table below.

Key Personnel **Project Manager**
Required Minimum Experience The contractor will ensure that the Project Manager has at least 10 years demonstrated experience in the following areas, which will be clearly reflected in resumes provided to the Government: • Strategic communications on behalf of a large public sector organization • Program management, including data collection and metrics development • Coordination with public and private sector stakeholders, to include state and local government, academia, law enforcement, and/or nongovernmental organizations ***Desired Experience*** In addition to the required minimum experience outlined above, additional experience for the Project Manager may be beneficial for task order work: • Community-based approaches to prevention (e.g., terrorism, public health, violence, etc.) • Social work, threat assessment, public health, policy analysis, or counterterrorism

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 listed below. The contractor shall not replace Key contractor personnel without acknowledgment from the Contracting Officer or Contracting Officer's Representative (COR).

5.3 Employee Identification

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times. Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

5.4 Employee Conduct

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist.

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status

is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times. Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

5.5 Removing Employees for Misconduct or Security Reasons

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

5.6 Data Rights

52.227-18 Rights in Data-Existing Works (DEC 2007)

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

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

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

(b) Allocation of Rights.

(1) The Government shall have-

(i) Unlimited rights in all data delivered under this contract, and in all data first produced in the performance of this contract, except as provided in paragraph (c) of this clause.

(ii) The right to limit assertion of copyright in data first produced in the performance of this contract, and to obtain assignment of copyright in that data, in accordance with paragraph (c)(1) of this clause.

(iii) The right to limit the release and use of certain data in accordance with paragraph (d) of this clause.

(2) The Contractor shall have, to the extent permission is granted in accordance with paragraph (c)(1) of this clause, the right to assert claim to copyright subsisting in data first produced in the performance of this contract.

(c) Copyright-

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

(i) The Contractor shall not assert or authorize others to assert any claim to copyright subsisting in any data first produced in the performance of this contract without prior written permission of the Contracting Officer. When copyright is asserted, the Contractor shall affix the appropriate copyright notice of 17 U.S.C. 401 or 402 and acknowledgment of Government sponsorship (including contract number) to the data when delivered to the Government, as well as when the data are published or deposited for registration as a published work in the U.S. Copyright Office. The Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license for all delivered data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

(ii) If the Government desires to obtain copyright in data first produced in the performance of this contract and permission has not been granted as set forth in paragraph (c)(1)(i) of this clause, the Contracting Officer shall direct the Contractor to assign (with or without registration), or obtain the assignment of, the copyright to the Government or its designated assignee.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract and that contain the copyright notice of 17 U.S.C. 401 or 402, unless the Contractor identifies such data and grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause.

(d) *Release and use restrictions.* Except as otherwise specifically provided for in this contract, the Contractor shall not use, release, reproduce, distribute, or publish any data first produced in the performance of this contract, nor authorize others to do so, without written permission of the Contracting Officer.

(e) *Indemnity.* The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability, including costs and expenses, incurred as the result of the violation of trade secrets, copyrights, or right of privacy or publicity, arising out of the creation, delivery, publication, or use of any data furnished under this contract; or any libelous or other unlawful matter contained in such data. The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to material furnished to the Contractor by the Government and incorporated in data to which this clause applies. (End of clause)

5.7 OTHER APPLICABLE CONDITIONS SECURITY

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

Requests for Exception to U.S. Citizenship Requirement
Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or through the DHS Office of the Chief Security Officer (OCSO). Components who have access may file their request via the Foreign National Vetting Management System (FNVMS), a part of the DHS OCSO Integrated Security Management System's (ISMS). For further information regarding the citizenship exception process, contact the DHS OCSO This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS
The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

(1) Carefully read the security clauses in the Order. Compliance with the security clauses in the contract is not optional.

(2) Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigation s will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office 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:

i. Standard Form 85P, "Questionnaire for Public Trust Positions"

ii. Standard Form 85P Certification

iii. Standard Form 85P Authorization for Release of Information

iv. FD Form 258, "Fingerprint Card" (2 copies)

v. DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"

vi. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Report Pursuant to the Fair Credit Reporting Act"

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

(2) 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 Security Office. No employee of the Contractor shall be allowed to access sensitive information or systems without a favorable EOD decision or suitability determination.

(3) 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 non-recurring meetings in order to begin transition work.

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

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

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

(7) Your POC at the Security Office is:

DHS OCSO/PSD Security Customer Service Center Telephone: (202) 447-5010
E-mailbox: officeofsecurity@dhs.gov.

5.8 DHS Cyber Requirements

FAR 52.224-3 Privacy Training – Alternate I (DEVIATION)

(a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at *http://www.dhs.gov/dhs-security-and-training-requirements-contractors*. Training shall be completed

within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

(End of clause)

HSAR Information Technology Security Awareness Training (HSAR Class Deviation 15-01) (JULY 2023)

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

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training

certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

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

(End of clause)