DEPARTMENT OF HOMELAND SECURITY (DHS)

STATEMENT OF WORK (SOW)
FOR
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)
EMERGENCY COMMUNICATIONS DIVISION (ECD)
INTEROPERABLE COMMUNICATIONS MARKETING INITIATIVE (ICMI)

1.1 Background

As the nation's premier cyber defense agency, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for leading the national effort to understand, manage, and reduce risk to the Nation's cyber and physical infrastructure. Interoperable communications failure is one of the most critical issues facing emergency responders and public safety today. To manage this risk, CISA collaborates with partners across all levels of government, public safety, national security/emergency preparedness, critical infrastructure, and industry to enhance resilient, interoperable, and secure emergency communications. CISA strives to improve the capability of the vital nationwide services to continue sharing information using emergency communications in day-to-day mission essential activities as well as during heightened incident support.

Title 6, United States Code (6 USC) Section 194(g)(1) defines the term "interoperable communications" as the ability of emergency response providers and relevant Federal, State, and local government agencies to be able to communicate with each other as necessary. 6 USC 571 (c)(12), 6 USC 571 (c)(13), 6 USC 572, 6 USC 573, 6 USC 574, 6 USC 575, 6 USC 576 and 6 USC 577 direct CISA to provide services, products, and support for the CISA mission, provide periodic updates to the National Emergency Communications Plan (NECP), and to track and measure national and state level progress in implementing NECP goals, recommendations, and initiatives. CISA services include, but are not limited to, provide technical guidance, training, and other assistance to ensure our partners in federal, state, local, tribal, and territorial governments, emergency response providers, the private sector critical infrastructure, and other organizations with emergency response capabilities achieve effective attainment of interoperable emergency communications. One service provided by CISA to enable effective emergency communication capability is the Priority Telecommunications Services (PTS) Program. Tools such as Wireless Priority Service (WPS) and Government Emergency Telecommunications Service (GETS) are provided as part of nationwide service offerings.

1.2 Scope

The overall scope of this professional services requirement is to obtain targeted brand management, marketing, public relations, and outreach services directed towards emergency communications experts throughout the United States and territories to be provided for CISA. These services will provide professional advice, outreach strategy development, focused brand management, marketing, public relations, and advertising capabilities (a wide-range of advertising formats (e.g., , print media, internet, and direct marketing)) necessary to promote PTS and other communication services of CISA by promoting interoperable communications

through strategic outreach to emergency communicators in critical infrastructure and within Federal, State, Local, Tribal, Territorial, and International (FSLTTI) Governments.

Tasks in this Statement of Work (SOW) refer to the ability for emergency officials to be able to communicate across all levels of Government and Industry, across all disciplines. The Contractor shall provide planning and advisory services for marketing, public relations, and outreach support to enhance the CISA strategic mission as it relates to emergency communications and priority telecommunications services. The Contractor will develop marketing strategies and planning to support the execution of programs for the following ECD missions:

- Integrated and Collaborative Communications Planning
- Priority Telecommunications Services (PTS)
- Emergency Communications Interoperability (ECI) Ambassador program (proposed)

No work in this SOW is associated with engineering or technology development of the Next Generation Network Priority Services acquisition program. There will be no Information Technology (IT) equipment or software developed or acquired on behalf of the program office. IT equipment, software, or networks supporting task deliverables are DHS provided. Any references to "cyber" are advisory only and incidental to the services outlined in this SOW.

1.3 Objective

Considering the evolving research landscape coupled with advanced technology and a wider array of effective marketing tools, CISA requires the development of brand management, marketing and outreach strategies that target specific groups of emergency communication personnel nationwide. CISA is seeking professional assistance in delivering a branding strategy and marketing communications plan that will provide:

- Development of strategic and external brand management strategy and marketing communications plans that are forward looking through 2033.
- Development of effective branding, marketing, public relations, and/or advertising strategies and tactics promoting internal and external culture change to the CISA target audience, aligned to the overall goal of Vision 2033.
- Development of a customer experience strategy to provide meaningful and focused messaging for emergency communications officials to create loyalty, enhance collaboration and partnership development, and retains an engaged community of practitioners.
- Develop and deliver a Program Management Plan through 2033 that defines tasks, timelines, internal and external resources required, and all associated costs to execute the strategies annually through 2033.
- Tools to reach a broader audience and increasing the number of qualified users of PTS services nationwide. The plan will be accomplished through the development of brand, marketing and outreach strategies along with the development of a program management plan with defined timeline defining objectives, deliverables, and cost estimates to achieve success by 2033.

The envisioned approach should include expanded online and social media presence, an array of awareness media options, an effective contact generation program, a nationwide support team providing advertising assistance through relevant local event activation, and the development of an Emergency Communications Interoperability (ECI) program and the design and distribution of program support materials.

1.4 Applicable Documents

a) 6 U.S.C. 571 - Office of Emergency Communications – http://www.gpo.gov/fdsys/granule/USCODE-2010-title6/USCODE-2010-title6-chap1-subchapXIII-sec571/content-detail.html
b) Homeland Security Act of 2002; Title XVIII – www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf
c) Executive Order 13618, July 6, 2012 – https://www.federalregister.gov/documents/2012/07/11/2012-17022/assignment-of-nationalsecurity-and-emergency-preparedness-communications-functions
d) Presidential Policy Directive-1(PPD-1) – https://fas.org/irp/offdocs/ppd/ppd-1.pdf
e) Office of Management and Budget M-07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007
f) DHS Handbook-Safeguard Sensitive Personally Identifiable Information, March 2012
g) DHS Privacy Incident Handling Guide, Version 3.0, January 26, 2012
h) National Emergency Communications Plan – https://www.cisa.gov/sites/default/files/publications/19_0924_CISA_ECD-NECP-2019_0.pdf
i) Congressional Research Service – Funding Emergency Communications: Technology and Policy Considerations – https://www.fas.org/sgp/crs/homesec/R41842.pdf
j) Middle Class Tax Relief and Job Creation Act of 2012 (the Spectrum Act) – http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-ll2publ96.pdf
k) Current and future versions of the Quadrennial Homeland Security Review – http://www.dhs.gov/guadrennial-homeland-security-review-ghsr
l) SAFECOM Grant Guidance – https://www.dhs.gov/safecom/blog/2017/06/09/fy-2017-safecom-guidance
m) The First Responder Network (FirstNet) and Next-Generation Communications for Public Safety: Issues for Congress (March 2014) – http://fas.org/sgp/crs/homesec/R42543.pdf
n) National Incident Management System – https://www.fema.gov/national-incident-management-system
o) National Response Framework – https://www.fema.gov/media-library/assets/documents/117791
p) Federal Emergency Management Agency. A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action – https://www.fema.gov/whole-community

q) The National Preparedness Goal – https://www.fema.gov/national-preparedness-goal
r) DHS Sensitive Systems Policy 4300A
s) DHS Security Architecture
t) DHS Sensitive System Configuration Guidance
u) NIST Publications including but not limited to SP 800-53 and 37.

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 Planning

2.1.1 Define a comprehensive messaging approach that harmonizes internal staff messaging and external messaging to current and prospective stakeholders, that unifies PTS awareness in all CISA outreach.

2.1.1.1 In collaboration with CISA staff and within 4 months of contract award, develop a plan to provide outreach strategy development, unified brand management, focused marketing, public relations, advertising capabilities and strategic outreach to officials within Federal, State, Local, Tribal, Territorial, and International (FSLTTI) Government and Critical Infrastructure Industry to promote PTS and other information and communication technology services of CISA.

2.1.1.2 Provide reporting on lessons learned (successes, issues, and any roadblocks encountered) in the development of the profile development task.

2.1.2 All the advertising materials and products produced under this contract shall be reviewed and shall require sign-off by CISA prior to distribution. This includes external communication products, which includes publications, multimedia products, graphics or other services produced through this contract as a deliverable:

2.1.2.1 Brochures and flyers;
2.1.2.2 Online publications;
2.1.2.3 Press releases, other media materials;
2.1.2.4 Other multimedia products;
2.1.2.5 Educational or information modules; and
2.1.2.6 Advertisement or Scripts for television, print, digital, social media, web, radio, mobile or any other specific media channel that will be recommended by the selected Contractor.

2.1.3 The Contractor may also prepare copy (written material), illustrative material (forms, etc.) and /or the "print ready" versions of creative products.

2.2 Branding and Advertising Strategy Development

2.2.1 Develop new CISA strategies focused on Brand Management, Marketing, Public Relations, Outreach, and Advertising Strategies.

2.2.2 Promote PTS and recommend new strategic outreach opportunities to the critical infrastructure community.

2.2.3 Develop detailed concept of the work required to include context, goals, objectives, target audiences, key messages, strategies, tactics, and performance measures.

2.2.4 The Branding and Advertising Strategy must include a detailed concept of all required services that must be tailored to specific audiences based on market research, to include the following as applicable:

2.2.5 Lead Generation Planning – provide solutions to identify prospects, strategic development of future leads, and development of emergency communications influencer strategies.

2.2.6 Awareness – recommend relevant public events, promotional programs, and other events that promote CISA objectives in this SOW, interoperable communications, and priority service awareness.

2.2.7 Customer Experience – perform appropriate customer experience research to understanding of customer goals, identify the current state of current experience, uncover areas for improvement, and determine customer needs during each stage of their lifecycle. Develop appropriate measures determine customer perception of the brand, their satisfaction with CISA offerings, and customer needs/values/expectations.

2.2.8 Support and Engagement Materials – define internal and external support services and requirements to accomplish the objectives in this SOW and the products recommended to achieve CISA goals.

2.2.9 Media and Advertisement Support – define creative development, media mix, paid media, and provide recommendations to achieve CISA goals.

2.3 Branding and Advertising Strategy Execution.

2.3.1 The Contractor must provide a strategic plan and roadmap to execute and maintain alignment with evolving CISA Branding, Marketing and Advertising Strategies.

2.3.2 An implementation plan is required, which will include the specific programmatic tasks required to accomplish the objectives, materials required, projected costs to complete, execution plan through 2030, and recommended external support requirements.

2.3.3 The Branding and Advertising Strategy must ensure all services are tailored to the specific audiences as identified through market research and CISA guidance, to include the following:

2.3.4 Branding and Advertising Strategy development that will document any internal process adjustments needed and the services that are required to provide support to the strategy, CISA objectives and initiatives. The strategies should provide plans to evaluate the effectiveness of the

Branding and Advertising Strategy and related tactics as initiatives are completed and as the it evolves. The Contractor must:

2.3.4.1 Develop an ECD Strategic Execution Plan to include creative concepts, alternative media plans, direct response programs, product positioning, short- and long-range communication objectives.

2.3.4.2 Provide advertising support recommendations. The Contractor's Branding and Advertising Strategy must be broad enough to accommodate the nuances and challenges of a nationwide outreach effort and maintain a consistent messaging.

2.3.4.3 Develop and deliver presentations that summarize recommended advertising efforts and objectives. Presentations may be in person, via conference call, or through video teleconference (VTC) and shall be used to brief CISA leadership and stakeholders in a concise manner during four quarterly briefings in a designated twelve-month period.

2.3.4.4 Perform quality assurance and control review of informational products prior to publication and final approval via the CISA Correspondence Action Task Tracker (CATT) advising with specific recommendations and suggested edits.

2.3.4.5 Coordination with the COR is required for all trademark reviews for any new slogan, logo, or other indicator.

2.4 Branding and Advertising Strategy Assessment

2.4.1 Develop and provide a Branding and Advertising Strategy Assessment.

2.4.2 Develop procedures to generate Qualified Leads for PTS. Qualified Leads are defined as vital nationwide service officials eligible for priority service tools (WPS/GETS).

2.4.3 Develop targeted lead generation products that encourage Qualified Leads to enroll in PTS.

2.4.4 Develop and execute direct response activities at the national, regional, and action officer levels that facilitate a call-to-action for prospects to seek immediate feedback from CISA.

2.4.5 Create a CISA influencer page, **https://www.cisa.gov.** This site collects requests for recruitment information and is the CISA's public facing portal. The intent of this website is to be appealing and useful to the primary target audience, influencers of such targets, and diversity targets. The COR or the Government official(s) designated by the COR will provide final approval for all content changes. The CISA retains all rights to this site including, but not limited to, all intellectual property rights related to, or associated with, the site.

2.4.6 Create an Advertising Portal (Ad Portal) and its subpages at https://adportal.cisa.com. This site is the access point for the following proposed support tools:

2.4.7 Social Media

2.4.7.1 Provide detailed plans to reach the target audiences through paid and organic advertising efforts.

2.4.7.2 Create content and programs to engage prospects and influencers that will call them to action, whether through service or support. The Government will provide all log-in information upon award. All posts, messages, account updates, and online activities on these accounts.

2.4.7.3 Awareness

2.4.7.3.1. Develop and execute public events and promotional programs that promote Emergency Communications Interoperability and PTS awareness.

2.4.7.3.2. Create useful opportunities for interaction with the target demographic.

2.4.7.3.3. Develop recommendations to execute and maintain a public relations campaign that includes developing and disseminating public service announcements (PSAs) and promotional and image-building initiatives through free media channels. The intent of this task is to enhance the CISA's image in the emergency communications field.

2.4.7.3.4. The Contractor must provide support for CISA as follows:

2.4.7.3.4.1. Develop and provide guides, sales tools, and pertinent marketing data.

2.4.7.3.4.2. Execute advertising and marketing initiatives in accordance with the Advertising Strategy.

2.4.8 Ambassador Program

Develop an Emergency Communications Interoperability Ambassador Program to recruit emergency communication officials from across the Nation to support the implementation of the strategic plan.

2.4.9 Advice and Coordination with Call Center

The CISA primary telephone number for support for national security/emergency preparedness users is 1-866-627-2255, which is staffed by the CISA Priority Telecommunications Service Center. Coordination of messaging by call center staff requires close advisory support to ensure alignment with the Advertising Strategy.

2.4.10 Paid Media

Distribute all media and advertisements under this contract via effective channels such as broadcast, digital (e.g., online advertising and software applications), audio, and printed

environments to maintain the established reach and engagement goals. Media and advertisements must reach 15% of the prospect audience at least two (2) times per month.

2.4.11 The Government will reimburse the Contractor only for the actual price paid for paid media, advertisements, royalty fees, and reoccurring charges associated with paid media and advertisements that are expressly identified as reimbursable items by this contract. Actual Price paid by the Contractor includes tax paid, if any, and reduced by all credits, rebates, and discounts whether accrued or realized, associated with the supplies and services provided. The Contractor shall seek exemption from taxes and rebates of taxes paid before including them in the Actual Price paid and shall inform the Contracting Officer of all instances in which the Contractor sought an exemption or rebate, and the taxing authority refused the request for an exemption or rebate. Actual Price does not include material handling charges, overhead, general, and administrative costs, profit, or any other indirect cost that is in any way associated with the Contractor's purchase or provision of the reimbursable item.

2.4.12 The Contracting Officer may reduce the reimbursement by any amount that the Contracting Officer finds, in his/her sole discretion, is greater than that which is fair and reasonable for the supplies or services provided, giving due consideration to the facts and circumstances prevailing at the time that the Contractor procured the supplies and services. Disputes as to the amount by which any reimbursement is reduced shall be resolved in accordance with the dispute's clause of the contract. It shall be the Contractor's burden to demonstrate that the price it paid for reimbursable items under this section is fair and reasonable. By submitting an invoice for Paid Media, the contractor certifies that the costs are fair and reasonable and in accordance with the terms of this section.

2.4.13 The Contractor shall not exceed or incur costs that exceed the amount of funding stated on a reimbursable CLIN. The Government is not obligated to reimburse the Contractor for an otherwise reimbursable item in excess of the funded amount stated on a reimbursable CLIN. The Government is not obligated to reimburse the Contractor for costs that are not allowable, allocable, and reasonable. The Contractor is not obligated to continue performance of any reimbursable work under this Contract or otherwise incur costs for reimbursable items in excess of the funded amount stated on a reimbursable CLIN unless the Contracting Officer notifies the Contractor in writing that the funded amount stated on the reimbursable CLIN has been increased. If notification is made verbally, such notification shall be followed up in writing within two (2) business days.

2.4.14 No notice, communication, or representation from any person other than the Contracting Officer shall affect the Government's obligation to reimburse the Contractor. Changes to the contract shall not be considered an authorization to exceed the funded amount stated on a reimbursable CLIN unless the change contains a statement expressly increasing the funded amount of the reimbursable CLIN by an enough to cover the change.

2.5 Contract Management. All plans must align with the CISA ECD's 2030 Strategy Plan.

2.5.1 Kickoff. The Contractor must schedule, coordinate, and host a Kick-Off Meeting within ten (10) days after the start of performance. The Government will provide the Contractor with the Meeting Agenda. The Contracting Officer's Representative (COR) will ensure all identified

participants are notified in advance of the meeting. The Contractor must develop and, after Government approval, distribute the Kick-Off Meeting.

2.5.2 Bi-Weekly progress meetings. Telephonic Progress Meetings are scheduled and conducted by the Government to evaluate current and prospective marketing, advertising, and stakeholder/partner/customer acquisition efforts. The Contractor must attend all Progress Meetings to provide insights, recommendations, and pertinent information that support meeting objectives. The Contractor must develop and, after Government approval, distribute Progress Meeting minutes.

2.5.3 Quarterly Progress. The contractor must develop a Quarterly Progress Report. Contractor shall brief the COR and Program Manager and other federal leads during the quarterly monthly meeting. Submission of the report will be submitted the first week of the quarter.

2.5.4 Quality Control Plan (QCP). The number of officials serving in the vital nationwide services change every year, and so the representation of one third representing leadership and the operational component necessary to perform mission essential activities. With consideration of these variables, the Contractor must develop and maintain a QCP that includes researched annual goals and Key Performance Indicators (KPIs). Copies of inspection documentation must be retained by the Contractor for the duration of this contract and must be available upon request by the government. Subsequent changes to the QCP shall be submitted to the COR no later than ten (10) business days prior to the effective date of change.

2.6 Material and Data Management. CISA desires to create a government library of assets to support its advertising and marketing strategies.

2.6.1 CISA Assets Library. The Contractor must store, organize, and catalog all advertising material (e.g., photographs, videos, print ads, etc.) created during the performance of this contract. The Contractor must create and maintain an Assets Library using available SharePoint tools. The Assets Library shall be available to the COR and any Government officials designated by the COR. The Contractor must ensure that all records abide by the intellectual property rights under this contract and remains searchable, compatible with CISA systems, and transferrable. The Contractor must maintain the original copies of all releases and licenses within the record. The Contractor must develop and maintain a digital Image and Video Content Rights Audit Sheet listing all such signed releases and licenses indexed to the products.

2.6.2 Inventory Management System. CISA's advertising and marketing inventory goal is to achieve a library comprised of collateral, recruiter support, promotional, and/or incentive items. The Contractor must maintain a full-time, self-service Inventory Management System using available SharePoint tools to facilitate warehousing and distribution for all items.

2.7 Surge

Additional surge marketing and advertising support may be necessary for the previously detailed tasks. When operational conditions require additional staffing and surge support, the contractor shall provide support, at the same hourly labor rate as specified under normal conditions, as

specified by the government. A minimum notice of thirty (30) days will be provided to the contractor prior to requesting and funding surge support line item(s). When such support is required, the government will specify the work to be performed, level of effort, and duration of assignment.

2.8 Transition Plan

The Contractor shall develop, document, and monitor the execution of a transition plan that may be used to transition tasks and materials to a new Contractor, or to the Government. The plan will incorporate an inventory of all services and materials developed that will be required to fully perform the services provided under this contract. The plan will include a schedule of briefings, including dates, times and resources allotted, that will be required to fully transition all materials developed to the follow-on Contractor, and will provide the names of individuals that will be responsible for fully briefing their follow-on counterparts. The plan is to ensure that the follow-on Contractor, or the Government, will be provided sufficient information and be fully briefed prior to the current expiration date of the contract, to provide adequate time for the new Contractor to have their personnel completely familiar with the requirements and in place on the turnover date. The Contractor shall plan for a thirty (30) business day(s) transition period. The plan shall provide the contact information for contractor individuals who will be assigned to the transition team and identify their roles in the transition. The Contractor shall participate in transition meetings with the program manager and project staff, and representatives of the successor Contractor. The purpose of these meetings is to review project materials and take preparatory steps to ensure an effective transition in Contractor support. The transition plan is due to the Government sixty (60) business days prior to the expiration date of the contract or as directed by the Government. The Contractor shall develop, document and monitor the execution of a transition plan that may be used to transition tasks and materials to a new Contractor, or to the Government. The plan will incorporate an inventory of all services and materials developed that will be required to fully perform the services provided under this contract. The plan will include a schedule of briefings, including dates, times and resources allotted, that will be required to fully transition all materials developed to the follow-on Contractor, and will provide the names of individuals that will be responsible for fully briefing their follow-on counterparts. The plan is to ensure that the follow- on Contractor, or the Government, will be provided sufficient information and be fully briefed prior to the current expiration date of the contract, to provide adequate time for the new Contractor to have their personnel completely familiar with the requirements and in place on the turnover date. The Contractor shall plan for a thirty (30) business day(s) transition period. The plan shall provide the contact information for contractor individuals who will be assigned to the transition team and identify their roles in the transition. The Contractor shall participate in transition meetings with the program manager and project staff, and representatives of the successor Contractor. The purpose of these meetings is to review project materials and take preparatory steps to ensure an effective transition in Contractor support. The transition plan is due to the Government sixty (60) business days prior to the expiration date of the contract or as directed by the Government. If the period of performance overlaps with an incumbent Contractor's efforts, the Contractor must collaborate with the incumbent Contractor to facilitate a successful transition-in. The Contractor's personnel must coordinate with the follow-on contractor's personnel to execute knowledge transfers; provide lessons learned; ensure continuity of information; transfer documents; and prevent gaps in service.

The Transition Plan must include the following:

- Program management processes;
- POCs;
- Location of technical and program management documentation;
- Appropriate Contractor-to-Contractor coordination to ensure a seamless transition;
- Schedules and milestones;
- Actions required of the Government;
- Effective communication procedures with the incoming Contractor and Government personnel for the period of the transition via weekly status meetings; and
- Assigned Contractor personnel that will conduct a joint inventory, including condition status assessments, with Government personnel of all advertising and promotional materials.

All facilities, equipment, and materials utilized by the Contractor personnel during performance shall remain accessible to the Contractor personnel during the transition period pursuant to the applicable in- processing and out-processing guidelines.

2.8.1 Task Execution
The Contractor shall develop a project plan for execution of task order activities. Scope, time, and cost elements shall detail work elements and deliverable items related to execution of ECD tasks.

3. CONTRACTOR PERSONNEL

3.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW. Personnel must have a proven track record in successfully performing work similar in size and scope to that outlined in the SOW. It is the responsibility of the contractor to propose qualified contractor personnel to perform all requirements specified in the SOW.

3.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is always maintained. The Contractor shall ensure that all contract support personnel are present for all hours 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.

3.3 Key Personnel

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed

substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as Key for this requirement. Note: The Government may designate additional Contractor personnel as *Key* at the time of award.

** Project Manager
** Creative Director

3.3.1 Minimum Qualifications for Project Manager

Project Manager - The Contractor shall provide a Project Manager responsible for all Contractor work under this SOW. The Project Manager shall possess at a minimum a MA/MS Degree and (10) years of experience to include excellent overall business and organizational skills with demonstrated success in achieving financial goals, managing multiple functions, managing relationships with clients, and providing quality service based on client requirements. Directs day-to-day management of contract support operations, possibly involving multiple tasks and groups of personnel at various locations or on a single project. Demonstrates skills in the scope of work of this SOW; provides technical guidance to the project team in the work performance and reviews the quality of all work products. Organizes, directs, and coordinates the planning and production of all contract support activities. Responsible for staffing, project planning, project financials, and staff direction and oversight. Assists senior management as required in managing contract performance.

The Project Manager shall be a single point of contact for the Contracting Officer and the COR. The Project Manager shall be one of the senior-level employees the Contractor provides for this work effort. The name of the Project Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Project Manager, shall be provided to the Government.

During any absence of the Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed for this SOW. Additionally, the Contractor shall not replace the Project Manager without prior approval from the Contracting Officer. The Project Manager is ultimately responsible for the Contractor's performance during the execution of the events workshops, briefings and meetings, to include logistics before, during, and after the events.

The Project Manager shall be available to the COR via telephone between the hours of 0730 and 1600 ET, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 24 hours of notification. Additionally, the Program Manager will notify the COR, by email or telephone, of any vacation, sick leave or appointment that would make said individual not available to the COR and the PM within days/hours listed.

3.3.2 Minimum Qualifications for Creative Director

Creative Director - The Contractor shall provide a Creative Director that shall possess at a minimum a bachelor's degree and (10) years of experience. Creative Directors will provide

creative guidance on all deliverables; works with Project Manager to develop high-level organization and campaign branding strategies; provides subject matter expertise and guidance on all traditional and multimedia deliverables; ensures high-level quality and appropriate formatting of all media and creative design products.

The Creative Director shall be available to the COR via telephone between the hours of 0730 and 1600 ET, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 24 hours of notification. Additionally, the Creative Director will notify the COR, by email or telephone, of any vacation, sick leave or appointment that would make said individual not available to the COR and the PM within days/hours listed.

3.4 Employee Identification

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

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

3.5 Employee Conduct

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

3.5.1 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.

OTHER APPLICABLE CONDITIONS

4.1 Security

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.

Contract employees waiting for an EOD decision shall begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by an authorized Contractor personnel or Government employee. This limited access is to allow Contractors to attend briefings, non-recurring meetings and begin transition work. All services provided will be in accordance with DHS Management Directive 4300.1 as implemented by DHS 4300A and/or 4300B Policies and Handbooks. Access to DHS IT Systems is governed by DHS 4300A, Sensitive Systems Policy, and DHS 4300 A, DHS National Security System Handbook.

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

All work performed under this SOW is Sensitive but Unclassified unless otherwise specified by DHS. This task order will require access to the following information (check all applicable boxes):

- Unclassified, no markings
- Sensitive but Unclassified (SBU), For Official Use Only (FOUO) Law Enforcement Sensitive (LES)
- Protected Critical Infrastructure Information (PCII) Confidential

1. All unclassified "For Official Use Only" (FOUO) work is expected to occur at the "medium" level per the NIST 800-60 (FIPS Security Categorization) and the Federal Information Security Management Act (FISMA). Any work at the "high" FOUO level per the FISMA, or any work at the classified level, shall be performed on a stand-alone computer system accredited in accordance with the FISMA and applicable DHS policies.
2. The Contractor shall comply with all requirements of the Protected CII (PCII) Program set out in the CII Act, in the implementing regulations published in the Interim Rule, and in the PCII

Procedures Manual as they may be amended from time to time and shall safeguard Protected CII in accordance with the procedures contained therein.
3. The Contractor shall ensure that each of its employees, consultants, and subcontractors who work on the PCII Program have executed Non-Disclosure Agreements (NDAs) in a form prescribed by the PCII Program Manager. The Contractor shall ensure that each of its employees, consultants and subcontractors has executed an NDA and agrees that none of its employees, consultants or sub- contractors shall be given access to Protected CII without having previously executed an NDA.
4. If classified work is required under this SOW, the Task Sponsor shall provide specific guidance to the ***Contractor*** as to which work will be conducted in a classified manner and at which classification level. If such DHS-guidance conflicts with other applicable guidelines (e.g., DOE, DOD, etc.), the Contractor shall adhere to the more stringent guidelines as determined by the DHS Task Sponsor and DHS Program Manager. The Contractor shall also adhere to other applicable Government orders, guides, and directives pertaining to classified or confidential work.

4.2 Security Requirements

4.2.1 Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive but Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

4.3 Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized COR, and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary 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 DHS

data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

4.4 Interconnection Security Agreements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

4.5 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.

- Carefully read the security clauses in the Order. Compliance with the security clauses in the contract is not optional.
- 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 everyone will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS 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:
    a) Standard Form 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
    d) Non-Disclosure Agreement"
    e) DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Rep01is Pursuant to the Fair Credit Reporting Act"
- 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.
- 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.

- 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.
- The DHS Security Office shall be notified of all terminations /resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.
- When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with department security policy are subject to having their access to Department IT systems and facilities terminated, whether the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).
- Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.
- The POC at the Security Office is:
  CISA Office of Security
  Personnel Security Staff
  Washington DC 20528
  Email: [redacted]

4.6 Period of Performance

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

Base Period	August 22, 2024 through April 21, 2025
Option Period One	April 22, 2025 through April 21, 2026
Option Period Two	April 22, 2026 through April 21, 2027

4.7 Place of Performance

The primary place of performance will be the Contractor's facilities with frequent visits to the Department of Homeland Security facilities in the Washington Metro Area.

4.8 Contractor Telecommuting – Remote Personal Residence Work Locations

Telecommuting for federal government contractors will be considered on a situational basis to the extent practicable to meet DHS mission needs. Telecommuting allows contractor personnel to perform their contractual requirements outside of CISA office locations, typically at a contractor's personal residence or a corporate telecommuting office location. Telecommuting for contractor personnel provides the government flexibility to meet unique CISA organizational and facility needs and requirements. The goal of telecommuting for contractor personnel is to enhance the delivery of services that support the DHS mission. Telecommuting is permitted under the task order in accordance with the requirements below.

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

4.9 Contractor Labor Rates Charged While Telecommuting

The contractor shall charge the same applicable fixed hourly rate as for a Government site for those contractor personnel when they telecommute at their designated telecommuting location.

4.10 Hours of Operation

Contractor employees shall generally perform all work between the hours of 0800 and 1700 EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW.

4.11 Travel

Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with the Federal Travel Regulations. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event.

4.12 Other Direct Costs (ODC)

The Contractor shall procure material/ODCs when essential to task performance and approved by the COR and the Contracting Officer. ODCs must be approved by the CO prior to incurring any costs. ODCs must be approved by the CO, and must be necessary, allowable, and allocable

for performance of this task order. ODCs must be submitted in enough time to the CO to give prior approval and must identify the purpose of the ODCs and provide a detailed cost breakdown. The contractor shall maintain the original or legible copy of receipts for all ODCs invoiced. All materials purchased by the Contractor for the use or on behalf of the Federal Government shall become the property of the Federal Government. The Contractor shall document the transfer of materials in addition to an account of all materials consumed during the performance of the task order. The Contractor shall furnish a copy of such documents at Quarterly Task Review Meetings.

4.13 Post Award Conference

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 15 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held at the Government's facility, located at 4200 Wilson Blvd. Arlington, VA or via teleconference.

4.14 Project Plan

The Contractor shall provide a WBS Project/Milestone Schedule prepared in MS Project at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than 30 business days after the Post Award Conference.

4.15 Original Business Continuity and Updated Business Continuity Plan
The Contractor shall provide an original Business Continuity Plan no later 15 calendars after date of award and the updated Business Continuity Plan during the quarterly progress report. The Contractor must develop and present. These plans will include prevention and recovery methods for potential threats to data such as natural disasters or cyber-attacks.

4.16 Progress Reports

The Contractor's Program Manager shall provide monthly task order and task performance progress reports to the Contracting Officer's Representative by noon, the fifteenth business day of each month via electronic mail. If the fifteenth business day of the month is a holiday, the report must be submitted by noon the following workday. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, and any travel conducted. Monthly reporting will reflect the actual cost and level of effort provided for each Program/Project must include actual burn rate charts and graphs, outline the expenditures, billings, work tasked/in-progress/completed during the month, deliverables submitted, work planned for the subsequent month, deliverables planned for the subsequent month, and any problems or issues encountered in contract or task performance.

4.17 Progress Meetings

The Contractor's Program Manager shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. The Program Manager shall present Quarterly Program Management Reviews each quarter, dates to be coordinated with the COR. These meetings shall take place at the Department of Homeland Security's Emergency Communications Division offices located in Arlington, VA or via teleconference.

4.18 General Report Requirements

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows XP and Microsoft Office Applications).

4.19 Protection of Information

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

The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

Contractor access to proprietary 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).

4.20 DHS and CISA ENTERPRISE ARCHITECTURE COMPLIANCE

All solutions and services shall meet DHS and CISA Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security Enterprise (HLS) Architecture (EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the CISA Chief Data Officer for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and CISA's Enterprise Data

Management Program Policy and all data-related artifacts will be developed and validated according to DHS and CISA data management architectural guidelines.

- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

4.21 DHS GEOSPATIAL INFORMATION SYSTEM TERMS AND CONDITIONS

All implementations including geospatial data, information, and services shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including (but not limited to) the following:

- All data built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Data Reference Model.

- All software built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Technical Reference Model.

4.22 EPEAT AND ENERGY STAR LANGUAGE

All hardware procured directly or in support of this action must meet applicable and appropriate Electronic Product Environmental Assessment Tool (EPEAT) and ENERGY Star standards.

4.23 DHS CYBER-SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) TERMS & CONDITIONS

a. Definitions

i. Component: a unit defined by the supplier that connects to and functions as part of the product. For software products, a component is a unit of software defined by a supplier at the time the component is built, packaged, or delivered. For hardware, a component is one hardware unit designed to connect to and function as part of a larger product.

ii. End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

iii. End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no

troubleshooting technical assistance will be offered).

iv. Information and Communications Technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

v. Product: part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.

b. Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product

i. The contractor shall provide new equipment unless otherwise formally approved by the Government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the Government. In the event that a shipped OEM product, or part or component of that product, fails, all replacements must be new (i.e., non-refurbished, not previously used) OEM.

ii. The contractor may provide previously-used OEM products only with written Government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

c. Accounting of Components in ICT Products

i. The contractor shall provide and maintain a list of components for each product used in performance of the contract, including through subcontracts or other arrangements. This list for each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.

ii. The contractor shall notify the Government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to reflect the new version of the software. This includes software builds to integrate an updated component or dependency.

iii. For software products, the contractor shall provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract, and replaced when End of Support (EoS) is reached.

iv. A contractor using team members in performance of the contract (e.g., subcontractors or other

service providers) shall ensure that the standards for the accounting of components in this subsection are met by team members.

d. Supply-Chain Transport

i. The contractor shall use formal, documented and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.

ii. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance, and make available for inspection upon request of the Government.

iii. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.

iv. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

v. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Changes to Ownership and Control

The Contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any significant changes to corporate ownership or control from contract award through final delivery or the end of the period of performance. A significant change would be one in which a change occurs in the individuals or entities who, directly or indirectly, either (1) exercises substantial control over an entity, or (2) owns or controls at least 25 percent of the ownership interests of an entity.

4.24 Section 508 Compliance

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

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508

Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05,

Section 508 Requirements for Technology Services

1. When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.
2. When modifying, installing, configuring or integrating commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.
3. When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The Contractor shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at https://www.dhs.gov/trusted-tester.
4. When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at https://www.dhs.gov/compliance-test-processes.
5. When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use

the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester

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

Section 508 Deliverables

1. **Section 508 Test Plans**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.
2. **Section 508 Test Results**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.
3. **Section 508 Accessibility Conformance Reports**: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.
4. **Other Section 508 Documentation:** The following documentation shall be provided upon request for ICT items offered through this contract:
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Documentation of core functions that cannot be accessed by persons with disabilities.
    - Documentation of remediation plans to address non-conformance to the Section 508 standards.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COR and a determination will be made in accordance with DHS Management Directives (MD) 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations

of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

4.25 THE HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12)

- The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to DHS facilities, networks, and information systems. Personal Identity Verification (PIV) credentials shall be used as the primary means of logical authentication for DHS sensitive systems. The Contractor must use his or her federal issued Personal Identity Verification (PIV) credentials to access DHS resources to include IT applications and physical facility.

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

4.26 ARTIFICIAL INTELLIGENCE/MACHINE LEARNING REQUIREMENTS

Definitions:

Artificial Intelligence (AI) includes the following: (1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks. (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task. (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

Requirements:

The 2019 National Defense Authorization Act (NDAA) and Executive Order (EO) 13960 require that AI used in the Federal Government foster public trust and confidence while protecting privacy, civil rights, civil liberties, and American values. All federal employees, contractors, and subcontractors, when designing, developing, acquiring, and/or using AI for or within DHS, will adhere to the following 9 principles.

1. Lawful and respectful of our Nation's values: Agencies shall design, develop, acquire, and use AI in a manner that exhibits due respect for our Nation's values and is consistent with the Constitution and all other applicable laws and policies, including those addressing privacy, civil rights, and civil liberties.

2. Purposeful and performance-driven: Agencies shall seek opportunities for designing, developing, acquiring, and using AI, where the benefits of doing so significantly outweigh the risks, and the risks can be assessed and managed.
3. Accurate, reliable, and effective: Agencies shall ensure that their application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective.

4. Safe, secure, and resilient: Agencies shall ensure the safety, security, and resiliency of their AI applications, including resilience when confronted with systematic vulnerabilities, adversarial manipulation, and other malicious exploitation.

5. Understandable: Agencies shall ensure that the operations and outcomes of their AI applications are sufficiently understandable by subject matter experts, users, and others, as appropriate.

6. Responsible and traceable: Agencies shall ensure that human roles and responsibilities are clearly defined, understood, and appropriately assigned for the design, development, acquisition, and use of AI. Agencies shall ensure that AI is used in a manner consistent with these Principles and the purposes for which each use of AI is intended. The design, development, acquisition, and use of AI, as well as relevant inputs and outputs of

particular AI applications, should be well documented and traceable, as appropriate and to the extent practicable.

7. Regularly monitored: Agencies shall ensure that their AI applications are regularly tested against these Principles. Mechanisms should be maintained to supersede, disengage, or deactivate existing applications of AI that demonstrate performance or outcomes that are inconsistent with their intended use or this order.

8. Transparent: Agencies shall be transparent in disclosing relevant information regarding their use of AI to appropriate stakeholders, including the Congress and the public, to the extent practicable and in accordance with applicable laws and policies, including with respect to the protection of privacy and of sensitive law enforcement, national security, and other protected information.

9. Accountable: Agencies shall be accountable for implementing and enforcing appropriate safeguards for the proper use and functioning of their applications of AI, and shall monitor, audit, and document compliance with those safeguards. Agencies shall provide appropriate training to all agency personnel responsible for the design, development, acquisition, and use of AI.

5.0 Government Terms & Definitions

Government Terms and Definitions can be located on Home Page | CISA and Home | Homeland Security (dhs.gov)

6.0 Government Furnished Resources

The Government will provide the workspace, equipment and supplies necessary to perform the on-site portion of Contractor services required in this contract, unless specifically stated otherwise in this work statement. The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer. The Contractor shall use Government furnished facilities, property, equipment and supplies only for the performance of work under this contract and shall be responsible for returning all Government furnished facilities, property, and equipment in good working condition, subject to normal wear and tear.

6.1 Property Inventory

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

6.2 Monthly Asset Management Report

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

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

6.3 Contractor Furnished Property

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in this SOW.

6.4 Invoices and Payment Provisions

Invoices shall be prepared in accordance with Attachment - 2 Terms & Conditions; Reference Attachment - 2 Terms & Conditions FAR Clause's 52.232-25 Prompt Payment, and FAR Clause 52.232-7, Payments under Time & Materials and Labor-Hours and 52.212-4 Alternate I Contract Terms and Conditions - Commercial Products and Commercial Services. In addition to invoice preparation as required by the FAR, Contractor's invoice shall include the following information:

1) Cover sheet identifying DHS;
2) Task Order Number;
3) Modification Number, if any;
4) DUNS Number;
5) Month services provided
6) CLIN and Accounting Classifications
7) ATTN: CISA/OUS
   - A. The contractor shall submit invoices monthly.
   - B. Contract Line Item Number (CLIN) and description for each billed item.
   - C. Any additional backup information as required by this contract.
   - D. The Contractor shall submit the invoice electronically to the address below: E-mail: NPPDInvoice.Consolidation@ice.dhs.gov
   - E. Simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

[redacted]

The contractor shall submit invoices to the email addresses above. Additionally, the contractor shall prepare and submit an enough and procurement regulatory compliant invoice and receiving report for technical certification of inspection/acceptance of services and approval for payment. The contractor shall attach back up information to the invoices and receiving reports substantiating all costs for services performed. The receiving agency's written or electronic acceptance by the COR and date of acceptance shall be included as part of the backup documentation.

If the invoice is submitted without all required back up documentation, the invoice shall be rejected. The Government reserves the right to have all invoices and backup documentation reviewed by the Contracting Officer prior to payment approval. Any receipts for purchase CISA property will be within 5 business days of purchase.

7 Government Acceptance Period

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions. The COR will have 7 business days to review deliverables and make comments. The Contractor shall have 5 business days to make corrections and redeliver. All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

8 Deliverables

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

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	4.14	**Post Award Conference**	NLT 15 Calendar days after Date of Award (DOA)	N/A

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
2	4.15	**Draft Contractor Project Plan**	At Post Award Conference	COR, Contracting Officer
3	4.15	**Final Contractor Project Plan**	30 Calendar Days After DOA	COR, Contracting Officer
4	4.16	**Original Business Continuity Plan**	NLT 15 calendars after date of award	COR, Contracting Officer
5	4.16	**Updated Business Continuity Plan**	During the Quarterly Progress Report	COR, Contracting Officer
6	4.17	**Progress Reports**	15th Business Day of the Month	COR, Contracting Officer
7	6.1	**Master Inventory Report**	Monthly with Progress Report	COR, APO
8	6.4	**Receipts for Purchased CISA Property**	Within 5 Business days of purchase	COR, APO
9	6.2	**Monthly Asset Management Report**	Monthly with Progress Report	COR, APO
10	6.2	**Invoices/packing slips/receipts for property purchased for CISA**	Monthly with the Asset Management Report	COR, APO
11	2.8	**Transition Plan**	60 Days Prior to Contract Expiration	COR, Contracting Officer
12	2.1	**Planning**	Within 4 months of contract award	COR, Contracting Officer
13	2.5.4	**Quality Control Plan** (Copies of inspection documentation must be retained by the Contractor for the duration of this contract and must be available upon request by the government)	First Draft at Post Award Conference Subsequent changes to the QCP shall be submitted to the COR no later than ten (10) business days prior to the effective date of change.	COR, Contracting Officer

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
14	2.2	**Branding and Advertising Strategy Development**	Within 3 months of contract award	COR, APO
15	2.3	**Branding and Advertising Strategy Execution**	Within 6 months of contract award	COR, APO
16	2.4	**Branding and Advertising Strategy Assessment**	Within 30 Days of Option Period One exercise	COR, APO

Tasks	Performance Standards	Acceptable Quality Level
Kick-Off	Submitted on time with attendees and action items.	< 1 request for revisions
Meeting Minutes	Submitted on time with attendees and action items.	< 1 request for revisions
Bi-Weekly Progress Meeting Minutes	Submitted on time with attendees and action items.	< 1 request for revisions for every 2 meetings
Quarterly Progress Report	Submitted on time and contains required information and points of contact.	< 2 revisions before final report
Quality Control Plan	Includes KPIs; recommendations to minimize mistakes and costs; a customer complaint feedback system; and RMP.	KPIs are met and problems encountered are minor and resolved in a satisfactory manner
Material and Data Management	On-Line Library ATO achieved within 20 months. ATO maintained and PII is secured; Inventory is catalogued and readily accessible to recruiters; < 12-hours downtime for any maintenance.	100% Compliance for ATO and PII; < 10 errors identified per review of the Inventory Management System; < 5% of orders delayed or incomplete per year

Tasks	Performance Standards	Acceptable Quality Level
Transition Plan	Prevents disruption or degradation of service in the event of a transition.	Meets all requirements and problems encountered are minor and resolved in a satisfactory manner
Advertising Strategy Execution	Services support CISA's Campaign Plan objectives and initiatives; Effectiveness is evaluated objectively, and recommendations are incorporated efficiently.	Meets all requirements and problems encountered are minor and resolved in a satisfactory manner
Lead Generation	Lead generation products and direct response activities in line with Campaign Plan objectives.	Meets all requirements and problems encountered are minor and resolved in a satisfactory manner
Awareness	< 12-hours downtime for any maintenance on recruitment web pages and Ad Portal; Public events and promotional programs promote Emergency Communications awareness and align with Campaign Plan objectives.	Meets all requirements and problems encountered are minor and resolved in a satisfactory manner
Ambassador Support	Ambassador guides, marketing tools, and training materials include pertinent marketing data Initiatives are executed on schedule.	Meets all requirements and problems encountered are minor and resolved in a satisfactory manner
Ambassador Support Materials	Developed IAW the Advertising Strategy.	< 5% rework per year
Media and Advertisement Support	Shipped and received on time.	> 90% of deadlines met per quarter
Paid Media	Media Schedules submitted on time and IAW the Advertising Strategy; Reaches 15% of the prospect audience at least two (2) times per month; Prices paid are fair and reasonable based on market data.	Meets required metrics and KPIs
Key Personnel	All Key Personnel meet minimum qualifications.	IAW SOW
GFP Inventory Report	Submitted on time and contains required information.	< 1 request for revisions
RMF compliance	Upgrades and updates to comply with emerging security requirements completed on time.	100% Compliance
Information Security	No data breaches or leaks.	100% Compliance