FEDERALLY FUNDED RESEARCH AND DEVELOPMENT (FFRDC) TECHNICAL EXECUTION PLAN (TEP)

U.S. Department of Homeland Security

Title: Educational Facility Threat-Hazard-Risk Analysis and Higher Education Safety & Security Needs Assessment

Component/Office: Mission and Capability Support (MCS)
Directorate/Division: Science and Technology Directorate
FFRDC: Homeland Security Operational Analysis Center (HSOAC)

Version: 1.1

Date: March 22, 2023

1. Challenge

As schools strive to fulfill their educational mission, one challenge they face is minimizing the risk of the range of threats both within and outside of school boundaries. The efforts of the education system to adapt to COVID-19 shed light on many new and emerging threats for schools, emphasizing the need for systems to be able to operate in both physical and virtual environments. As such, there is a critical need to understand the evolving landscape of needs and threats education faces as well as what capacity-building (and scalable) resources are needed to support schools in how they approach their security and safety practices.

Although hazard and threat assessment (and risk analysis to prioritize among many possible damaging incidents) is the first step of security planning, primary and secondary (kindergarten – grade 12) school staff do not always have the time and needed expertise to assess both current and emerging threats to inform their preparedness and security planning, potentially hindering their ability to manage the variety of risks affecting their school communities efficiently and effectively.

Post-secondary educational institutions have their own safety and security challenges, some of which are common with primary and secondary schools but others distinct to the nature of college and university campuses and student populations. Though they often have greater expertise and resources than local schools, colleges and universities also have competing requirements for funds and staff time which can challenge their efforts to protect their facilities and communities. The diversity of such institutions adds to the challenge: large schools can be tasked with protecting populations rivaling small cities as they host major sporting or other

events, while the safety and security challenges that smaller or more rural schools face may be more contained and involve the protection of fewer facilities and people.

2. Outcome(s)

The effort will yield two outcomes: (1) the creation of an online assessment tool that will enable individual educational institutions (or school systems) to explore the range of threats and hazards they face locally, to view a prioritization of these threats and hazards according to the risk that each pose, and to make informed estimates about what is most important for their safety and security planning. This tool will complement other available tools as well as safety and security guidance to enable local educational organizations to make better resource and planning decisions for their schools; and (2) the writing of a report exploring and summarizing higher education safety and security needs and requirements, building on previous work on primary and secondary school protection.

3. Background

Since 2020, the Cybersecurity and Infrastructure Security Agency's (CISA) School Safety Task Force (SSTF) has worked with HSOAC to develop the 3rd edition of the K-*12 School Security Guide* and *School Survey*. The K-12 School Security Product suite provides K-12 schools with the doctrine and methodology necessary to implement a layered, systems-based approach to school physical security. Additionally, the suite includes an interactive tool for conducting vulnerability analysis with respect to specific threat scenarios and outlines existing safety and security measures to help identify attractive strategies and options for improving physical security at their facilities. HSOAC has also supported the development of guidance for schools around encouraging students and community members to report potential threats and other student or staff safety concerns to enable intervention before incidents occur. In ongoing work, HSOAC is examining threats of school violence posted on social media to bridge the online and physical realms of school safety in K-12 schools. Assessing and responding to such threats has challenged school systems across the country in recent years.

However, there are several areas of support to school safety planning that these efforts have not addressed. First, while the online *School Survey* (renamed the *School Security Assessment Tool* or SSAT) provides users with a broad choice of scenarios (ranging from active assailants staging attacks inside the school to individually focused threats like a noncustodial parent attempting to kidnap a child), it does not help inform the user's choice of scenarios to use in assessing their security efforts. Depending on a school's individual environment, some threats may be more likely or potentially more damaging than others, and therefore should be prioritized in planning and assessment. While there are some existing tools and resources that guide security planners (at schools and more broadly) using risk assessment to make those choices, many assume a level of knowledge and time commitment that may not be realistic for all educational organizations. Past work has also focused primarily on physical security

planning (and therefore on threats of violence), and as such has not helped schools consider diverse threats in the context of natural, technological, and other hazards.

Second, HSOAC's work with CISA SSTF also focused on the safety and security needs of K-12 schools and has not yet examined the safety and security needs of higher education institutions. With the recent passage of the Safer Communities Act, and implementation of the Luke and Alex School Safety Act, additional responsibilities will be required, including efforts focused on higher education. As a result, insight into this area will be relevant to CISA, and the Federal School Safety Clearinghouse's, future efforts.

4. Task Objective(s)

The objectives of this task are twofold:

- Creation of an online threat, hazard, and risk assessment tool that will allow an individual school or school district security planner to quickly assess the level of violence threat, natural hazards, technological hazards, and cyber threats to their institution, informed by available data sources and local conditions.
- Development of a written report exploring and summarizing higher education safety and security needs and requirements.

5. Technical Approach / Analytic Methodology

5.1 Online Threat, Hazard and Risk Assessment Tool Development

5.1.1 Literature, Existing Assessment Tool, and Needs Review

Building on the results of previously completed scoping efforts, the research team will review available literature and existing risk assessment tools across the education and other sectors to provide the foundation for tool development. To meet local requirements, the research team will seek out both existing information and design options for combining the results from broad datasets (e.g., natural hazard or school violent incident data assembled at the national level) with local information necessary to customize threat/hazard assessment results. To inform development, the research team will consult with individuals representing the eventual tool's potential end user base, as well as other subject matter experts as needed.

5.1.2 Threat, Hazard and Risk Dataset Identification and Assembly

The research team will identify and collect existing datasets describing the threats and hazards that educational institutions should consider in their safety and security planning. The threats and hazards will include: violent threats to schools, natural hazards (e.g., earthquake, flooding), technological hazards (e.g., hazardous materials transport near school facilities), and cyber threats. Existing datasets will be identified and sourced from government (e.g., FEMA) and other sources (e.g., open source or other available datasets on school violence such as National

Center for Education Statistics data). For threats where incident or occurrence data is likely more difficult to obtain (e.g., cyber threats), the research team will develop practical and accessible ways for users to estimate those threats and risks. All datasets will serve as the foundation for individual users to estimate probabilities of occurrence and potential consequences (and therefore risk) from different threats or hazards in their specific area. The team will identify how to summarize or abstract relevant details from the datasets for inclusion in the eventual online tool.

5.1.3 Geospatial Data Analysis for Tool Development

To go beyond many existing approaches to risk assessment, the HSOAC research team will explore ways to use geospatial analysis and projection of future trends in threats and hazards to inform tool development. Given the evolution of threats and hazards over time, this type of analysis is critical for building a tool that does not lock planning into historically observed trends. This line of effort will involve two main subtasks, focusing on threats of violence and other hazards respectively.

- For threats of violence, the research team will use geospatial analysis to identify risk factors for *threatened, attempted, and completed* school violence incidents. This effort will use existing databases in combination with news reports and other sources to assemble as broad a geographic picture of school violence risk as possible. Somewhat paralleling the approach applied to identifying individual risk factors for violence (see e.g., United States Secret Service analyses of groups of school violence incidents), the HSOAC research team will explore geographic risk factors for violence using data on school characteristics, U.S. Census data on local geography, local crime data, and other data sources. This approach will contribute to efforts to build a set of geographic risk factors of risk of attempted violence, which can then be used to customize results for tool users in a specific geographic area. This adapts the approach used in a recent DHS START Emeritus COE analysis of domestic terrorism risk.[1]

- For other risks, the research team will seek out analytical approaches to project how different hazards may shift over time (e.g., increased probability of flooding in coastal areas over time). To the extent that existing data sources already have done this type of extrapolation, we will draw on them. If existing data do not meet our needs, we will develop ways for users to perform reasonable sensitivity analyses for potential hazard trajectories going forward.

---

[1] Boyd, Marcus A. and Samuel Henkin, "Alternative Scales of Extremism: The Relationship Between Scale and Predictive Measures of Extremism in the United States," Final Report. College Park, MD: START, 2022.

5.1.4 Tool Development

Building on the process used by CISA and HSOAC in the development of the SSAT, HSOAC research and programming staff will develop an online tool intended for deployment on CISA.gov. Development will be guided by collaboration with CISA and the relevant Component IT staff, to ensure programming within a compatible and deployable web development architecture. Though the exact feature set, interface, and other details of the tool will be developed over the course of the project, the core goal is a design that (a) allows a user to perform a threat, hazard, and risk assessment for their specific geographic data based on available data; (b) enables customization or entry of local level insights or data to utilize user knowledge beyond what is available in existing datasets; and (c) covers and compares risks from violence, natural hazards, technological hazards, and cyber activities.

5.1.5 User Feedback

Analogous to the process used in the development of the SSAT, HSOAC assumes that CISA will want to carry out a user feedback process when the tool is in the later stages of development (but prior to completion). HSOAC will support this process and work to incorporate feedback before final tool completion.

5.1.6 Tool Documentation

HSOAC will document the task and its productions in four ways: (a) an HSOAC publication summarizing the existing literature and the threat/hazard/risk assessment process that informs the associated doctrine and tool; (b) a draft threat/hazard/risk assessment doctrine publication supporting CISA's development of a U.S. Government publication related to the tool; (c) a user guide describing the tool and providing instructions for its usage; and (d) a technical appendix that transparently lays out the workings of the tool and the steps involved in assembling the data it returns to users.

5.1.7 Tool Transition and Roll Out

HSOAC will prepare the threat/hazard/risk tool for transition to CISA.gov and assist in that process before tool release.

5.2 Higher Education Safety & Security Needs Assessment

5.2.1 Landscape and Literature Review

HSOAC will review existing published literature on the nature of threats, safety concerns, and hazards relevant to the higher education sector. As relevant, existing violent incident datasets will be explored to assess available data on campus violence and sources identified in the Task 5.1.1 literature search relating to higher education institutions will be drawn upon. The research team will also review available data on other forms of campus crime, as well as

information regarding institutions of higher education experience with natural or technological disasters.

HSOAC will review existing assessments of campus safety and security requirements as well as assessments of campus preparedness to inform a baseline picture of potential needs. The review will also examine existing planning tools to assess the need for development of new resources or tools to support planning in this sector.

Whenever possible, the review will draw on existing work and resources collected in prior or ongoing HSOAC research for CISA on K-12 school safety and security.

5.2.2 Focused Stakeholder, Subject Matter Expert Interaction, and Site Visits

The results of the landscape and literature review will be used to structure a focused stakeholder discussion that will complete the picture of threats/hazards, vulnerabilities, and needs in higher education. HSOAC will design this effort based on similar (likely virtual) feedback sessions conducted with K-12 education stakeholders to elicit insights from stakeholders and other relevant SMEs.[2] Participants will be expected to provide feedback on the priorities identified in Task 5.2.1 to shape the eventual product resulting from this task.

Because of the nature of this topic area, site visits to selected institutions of higher education may be a very effective way to collect information to flesh out the needs assessment. Though some local universities in the cities of residence of staff could potentially be visited, this task plans travel for four site visits to diverse colleges and universities (e.g., covering large and small institutions in both urban and rural locations).

5.2.3 Documentation of Results

The results of the review and stakeholder feedback will be documented in a published HSOAC report that identifies key security and safety risks to higher education campuses and describes current preparedness and security approaches. The findings of the assessment will be used to frame potential recommendations for improvement, assess the need for tools focused on higher education similar to those developed by HSOAC for CISA to assist K-12 safety and security planning, and recommend opportunities for DHS to contribute to safety and security in the sector.

6. Key Words

Security planning, all-hazards, school safety, school security, preparedness, higher education, colleges, universities

---

[2] See work described in Moore, Pauline et al., *Supporting Individual Willingness to Report School Safety Concerns: Findings from the Literature and Interviews with Stakeholders Across the K–12 School Community*, Santa Monica, Calif., RAND Corporation, 2022, https://www.rand.org/pubs/research_reports/RRA1077-3.html.

Type of Work

Literature review, expert assessment, data analysis, online tool development

Benefit of Work

Improve safety and security of primary, secondary, and post-secondary educational institutions

Subject of Interest

School Safety and Security

7. Focus Area and Mission Alignment

Table 1 below aligns the percent of the total projected Staff Years of Technical Effort (STE) allocations to the IDIQ focus areas and DHS Quadrennial Homeland Security Review (QHSR) missions.

HSOAC proposed total STE: 2.93

DHS Management Directive 143-04, "Establishing or Contracting with FFRDCs and National Laboratories" defines a STE as 1,810 hours of paid effort for technical services.

Table 1: Focus Areas to the QHSR Mission Areas Relationship Matrix

HSOAC Focus Areas	Mission 1: Prevent Terrorism and Enhance Security	Mission 2: Secure and Manage Our Borders	Mission 3: Enforce and Administer Our Immigration Laws	Mission 4: Safeguard and Secure Cyberspace	Mission 5: Strengthen National Preparedness and Resilience	Mission 6: Maturing and Strengthening Homeland Security
1: Acquisition Studies	0%	0%	0%	0%	0%	0%
2: Preparedness, Response, and Recovery	13%	0%	0%	7%	13%	0%
3: Innovation and Technology Acceleration	0%	0%	0%	0%	0%	0%
4: Homeland Security Threat and Opportunity Studies	14%	0%	0%	7%	13%	0%
5: Personnel Policy and Management Studies	0%	0%	0%	0%	0%	0%
6: Operational Studies	13%	0%	0%	7%	13%	0%
7: Organizational Studies	0%	0%	0%	0%	0%	0%

8: Regulatory, Doctrine, and Policy Studies	0%	0%	0%	0%	0%	0%
9: Research and Development Studies	0%	0%	0%	0%	0%	0%

8. Deliverables and Schedule

The HSOAC shall provide the following deliverables (predicated in calendar days), according to Table 2 below, and the most current Project Management Plan (PMP), as approved by the Project Manager and DHS Contracting Officer or Contracting Officer's Representative (COR).

Table 2: Deliverables

Scope Ref.	Deliverable Name	Delivery Date
5.0.1	Project Management Plan (PMP) (Draft)	15 calendar days after award
5.0.2	Project Management Plan (PMP) (Final)	30 calendar days after award
5.0.3	Task Order Project Kickoff Briefing	Within 30 calendar days of project award date
5.1.1, 5.1.2, 5.1.3, 5.2.1	Client Literature, Data and Analytic Check-in Meetings (CISA/S&T as desired)	Every two weeks starting after project kickoff meeting.
5.1.4	Client Tool Development Design Check-in Meetings (CISA/S&T as desired)	Every (alternating) two weeks starting after design efforts begun (estimated 4 months from project award date or from approval of initiation of all data collection, whichever is later).
5.2.2	Higher Education Stakeholder Interaction	9 months from project award date or from approval of initiation of all data collection, whichever is later.
5.1.5	Tool User Feedback Sessions	Scheduled at CISA's discretion (estimated 12 months from project award date or from approval of initiation of all data collection, whichever is later)
5.2.3	Draft HSOAC Higher Education Report	12 months from project award date or from approval of

		initiation of all data collection, whichever is later.
5.1.6	Draft HSOAC Threat/Hazard/Risk Report	14 months from project award date or from approval of initiation of all data collection, whichever is later.
5.1.6	Draft Doctrine and Tool Documentation	16 months from project award date or from approval of initiation of all data collection, whichever is later.
5.2.3	Final HSOAC Higher Education Report (ready for publication)	16 months from project award date or from approval of initiation of all data collection, whichever is later
5.1.6	Final HSOAC Threat/Hazard/Risk Report (ready for publication)	18 months from project award date or from approval of initiation of all data collection, whichever is later.
5.1.6	Revised Draft Doctrine and Tool Documentation	19 months from project award date or from approval of initiation of all data collection, whichever is later.
N/A	Final Task Completion Memo – Final documentation of deliverables and summary of work performed since final report delivered.	24 months from project award date or from approval of initiation of all data collection, whichever is later.

The HSOAC shall provide all deliverables under this task order directly to the S&T HSOAC PMO (via [redacted] the Task Order PM, TPOCs, and Task Order COR. An unclassified abstract, 100 to 200 words in length, and at least five keywords, or a completed Standard Form 298, "Report Documentation Page," shall accompany each deliverable as indicated in Table 2 deliverable. Note that the Report Documentation Page will identify the approved release distribution level (e.g., distribution is unlimited; distribution authorized to US Government agencies only; etc.).

The HSOAC shall deliver a monthly status report by the 15th for HSOAC of the following month containing metrics pertaining to financial, schedule, technical progress, deliverable status, and risk information related to the task. The HSOAC task lead and the task order COR as needed will discuss relevant issues in evaluating the task priorities for the next period; and update the program plan as necessary.

9. Assumptions

HSOAC considers this project to be non-severable. The nature and scope of HSOAC projects makes categorization of them as non-severable most appropriate. A non-severable undertaking constitutes a specific, entire job or single undertaking with a defined end-product (such as a final report of research) that cannot feasibly be subdivided for separate performance.

Staff working on HSOAC projects receive Fitness/Suitability, PIV/badges, DHS headquarters IT access, and security clearances under the IDIQ contract rather than having to wait to be cleared under each task order. This helps to ensure that the HSOAC can agilely respond to requirements and apply the full advantages that its open matrix structure provides the Department. It also saves the government valuable resources by leveraging active access and current investigations rather than performing additional investigations. This is keeping with the spirit of DHS Instruction 121-01-007-01, which states in part that "Reciprocity applies to the fullest extent possible" and "investigations and adjudications conducted by other federal agencies should be used whenever practicable to reduce the number of investigation requests, associated costs and unnecessary delays." We assume that the sponsor will offer reciprocity of the Fitness they have through our primary sponsor, as is customary.

10. Travel

Travel may be necessary to meet and coordinate interagency exchanges of information and to collect data for this task. The HSOAC shall provide trip reports, if requested, to the task order COR for all non-local travel within 30 days of completion of travel.

Long Distance Travel

From	To	No. of Trips	No. of Days per Trip
Eagle, Colorado	Washington, DC	2	3
Eagle, Colorado	Various [site visits]	4	2
Washington, DC	Various [site visits]	4	2

- Total Number of Trips (All Travelers): 10
- Total Number of Travel Days (All Travelers): 22

The task order COR must approve all foreign travel. Foreign travel must be approved at least 30 days (for unclassified visits) or 45 days (for classified visits) in advance of the planned travel event.

Travel, including local non-commuting travel, shall be reimbursed in accordance with the Federal Travel Regulation. Daily commuting costs shall not be reimbursed. Long-distance travel not specified in this Task Order must be pre-approved by the Task Order CO or COR.

11. Period of Performance

The period of performance is 24 months from date of task order award.

Note: The HSOAC IDIQ contract limits task order end dates to 3/23/2028. Also, options and addons cannot be executed on the current IDIQ contract on pre-existing task orders after the IDIQ end date, 3/23/2027.

12. Security Requirements.

This Task Order will require access to the following information

- ☒ 1. Unclassified, no markings
- ☒ 4. Personally Identifiable Information (PII)

12.1 The contractor shall use Science & Technology or another DHS Components' accredited General Support System (GSS) to accomplish this work, when applicable, until such time as HSSEDI or HSOAC Accredited Enclave solution becomes available. If classified work is required under this Task Order, the Task Order COR shall provide specific guidance to the HSOAC 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 HSOAC shall adhere to the more stringent guidelines as determined by the Task Order COR and DHS HSOAC PMO. The HSOAC shall also adhere to other applicable government orders, guides, and directives pertaining to classified or confidential work.

12.2 Authorized IT Environments

The HSOAC team will use their HSOAC corporate IT environment for HSOAC contracts management and administrative support for activities including:

- Time reporting
- Financial management
- Contract management
- Monthly status reports
- Non-DHS Sensitive project work

Sensitive HSOAC work described in the TEP will be performed in IT environment(s) authorized by DHS. These may include, a) HSOAC IT Enclave (following ATO by DHS), b) DHS infrastructure (e.g., LAN-A), and/or c) other authorized environment(s)(e.g., classified networks).

12.3 DHS Furnished Information

HSOAC does not anticipate that DHS-Furnished Information will be required for completion of this task order.

12.4 HSOAC Furnished Information

HSOAC does not anticipate that any unique HSOAC-Furnished Information will be involved in completion of this task order.

12.5 Privacy Compliance Requirements

The Government Program Manager will coordinate with the appropriate DHS component's Privacy Office (i.e., CBP, USCIS, S&T, etc.) to determine if a Privacy Threshold Analysis (PTA) is required prior to the start of performance. In those instances, the performer shall support the development of compliance related documentation and meet privacy requirements. Please have your privacy office reach out to S&T Privacy to see what documentation is available.

13. Safeguarding/Storage:

a. No safeguarding/storage needed at the HSOAC.

14. Other Contract Details

In accordance with the language in the HSOAC contract, the following sections are repeated here for awareness and should not be changed. If they are changed, the language in the IDIQ takes precedence.

14.1 HSOAC Personnel

Personnel provided by the HSOAC will have the skills and technical background necessary to successfully complete the tasks described in this plan. The HSOAC shall implement and manage the technical approach, organizational resources, management, and quality controls to be employed to meet the cost, performance, and schedule requirements throughout task order execution.

14.2 Food and Drink.

The HSOAC shall not charge any expense for food, snacks, or drink as part of holding task related meetings, conferences, or gatherings; however, this prohibition does not prevent the contractor from charging meals and incidental expenses as part of authorized travel expenses.

14.3 Meetings and Workshops

All necessary conference approvals should take place prior to the HSOAC's attendance at any conference in support of the sponsoring component. The component user should follow the conference approval process per the guidance set-forth under DHS Financial Management Policy Manual (FMPM Section 7.10) and any component-specific policies and procedures and provide a copy approval(s) to the HSOAC.

The HSOAC may interview and conduct workshops of recognized subject-matter experts, including non-federal experts, to gather the expert's individual knowledge and experience regarding the current state of the art of the technical issues relating to this task, and to foster the building of a long-term collaboration between the individual subject matter experts and the HSOAC on the issues relating to the experts' areas of expertise. The workshops or other interaction with non-Federal experts will be for the purpose of collecting the views of the individual experts, not to result in a consensus of those experts. The HSOAC shall produce an objective assessment on the technical merits of the data and/or experts' views espoused in these meetings; and include an evaluation of the strengths and weaknesses of the various discussion points provided by individuals.

The HSOAC may organize meetings/workshops related to the task with federal officials on behalf of the user; however, federal government personnel will approve the agenda and will chair any federal intra-agency/inter-agency meetings. The HSOAC shall produce an objective assessment on the technical merits of individual and any consensus findings and recommendations discussed in these meetings; and include an evaluation of their strengths and weaknesses of the various discussion points.

14.4 Inherently Governmental Functions

As defined under FAR subpart 7.503 (d) and additionally as described in the Office of Federal Procurement Policy (OFPP) Letter 11- 0 I, Performance of Inherently Governmental and Critical Functions (76 Fed Reg 56227), the HSOAC may perform certain closely associated with inherently Governmental functions. However, in accordance with Federal Acquisition Regulation (FAR) 7.503(c)(20) and Homeland Security Acquisition Manual 3037.103(e), the HSOAC shall not draft Congressional testimony, responses to Congressional correspondence, or agency responses to audit reports from the Inspector General, the Government Accountability Office, or other Federal audit entity. Furthermore, in accordance with FAR 7.503(c)(12)(ii), HSOAC employees, subcontractors, and/or consultants will not be voting members on any DHS source selections. When applicable, FAR clause 52.203-16, "Preventing Personal Conflicts of Interest," as included in the IDIQ contract, will apply to this Task Order.

14.5 Out of Scope Work

The following types of work are out of scope for the HSOAC to perform. More specific types of work that are out of scope are found in the relevant IDIQ contract:

- Performance of any services and functions as defined under FAR Subpart 7.5 - "Inherently Governmental Functions," specifically subparts 7.503 (a), (b) and (c).

- Performance of any Systems Engineering and Technical Assistance (SETA) type work, particularly where such work is directly for staff augmentation and of a general support nature where the specific type and quantity of deliverables are undefined.
- Preparation of any Independent Government Cost Estimates (IGCEs).
- Participation in any Source Selection Evaluation or any other membership body where voting and/or ranking of proposals will lead to a subsequent monetary or contract award. The HSOAC may provide independent technical evaluation of proposals in support to a Source Selection Evaluation body but may not provide any ranking, voting or other assigned ordering or selection criteria other than commenting on the technical merit of a particular proposal or proposal section(s). Use of the HSOAC in evaluating an offeror's proposal MUST BE DISCLOSED IN THE SOLICITATION OF PROPOSALS and the offeror(s) given the opportunity to affect non-disclosure agreements and/or withdraw their offer(s), otherwise the HSOAC may not participate.
- Delivering recurring compliance training to DHS employees, particularly that which could reasonably be considered staff augmentation services, is not allowed. Training associated with the transfer of skills from the HSOAC to DHS is acceptable, as long as such training is non-recurring (i.e., train the trainer) and is not intended to be part of a formal established training program. Waivers to this may be requested from the HSOAC COR. Seminars, workshops, and short courses intended to extend the access and awareness of HSOAC research, research methods, and data sets to practitioners across the Homeland Security Enterprise to assist them in improving mission effectiveness and efficiency is permissible.
- Software and/or hardware development or other manufacturing unless such development is associated with a prototype demonstration or other proof of concept system and not intended to be a permanent solution or in response to formal requirements.

15. Publications and Communications Concerning Work Performed

In accordance with the language in the HSOAC contract, the following statement is repeated here for awareness and should not be changed. If it is changed, the language in the IDIQ takes precedence.

The HSOAC shall mark all technical data or computer software pursuant to the terms of the IDIQ Contract. This will include, for copyrighted works, an appropriate notice acknowledging DHS's sponsorship of the work, license rights, and the appropriate copyright notice as detailed in the IDIQ Contract.

The DHS desires widespread dissemination of the results of funded non-sensitive research and does not seek to undermine the independence or objectivity of the HSOAC or HSOAC operator

in anyway. The HSOAC therefore will generally seek public release approval for the results of non-sensitive research. Thirty (30) days prior to release, the HSOAC will first ask for the task order COR's and CO's agreement that the research product is suitable for release. The HSOAC contract governs the scope of the review. Specifically, this review is strictly a mechanism by which the Department identifies the inclusion of Sensitive Information, as defined in the IDIQ contract, Section I.13(a). The review does not include a determination of the HSOAC's analytical conclusions, final findings, or analytical outcomes.

- Are you interested in releasing information publicly from this research?
  Yes.

- If you don't want to release the results, is the HSOAC able to release info about the methodology to the other components or the public?
  N/A

- What is the desired audience for the release of info? Component only/all of DHS/public release?
  As outlined in this TEP, there are variety of audiences for the results of this work and descriptions of the methodologies used. These include the sponsoring office, CISA, partners in the School Safety Task Force, and non-federal and private educational agencies and institutions from the local to regional levels. The sponsor will work with HSOAC as part of the planning process to develop a dissemination strategy that shares results appropriately for the relevant audiences.

- Do you want an outreach event as part of the release?
  To increase the benefit of the work and accompany release of results, the sponsor is interested in developing a plan to share the results with appropriate audiences. To accomplish this, the sponsor will work with HSOAC to develop an appropriate dissemination strategy that will support accomplishment of the objectives outlined in this TEP. Examples of components of a dissemination strategy could include briefings of results to DHS leadership within the sponsor's agency, HSOAC or DHS press releases to accompany release of non-DHS sensitive results or methodology developments, presentations at relevant associations or industry events, and/or HSOAC or DHS hosted meetings or symposia. The specific elements of the dissemination strategy will be determined during the planning process throughout the study.

- Would you be interested in having the PMO assist with the release of favorable results?
  To increase the benefit of this work, the sponsor welcomes assistance from the PMO to complement HSOAC and sponsor dissemination of results. As dissemination planning proceeds throughout the study, the sponsor will work with HSOAC to identify

opportunities to leverage the PMO to enhance the dissemination strategy and include the PMO into the planning process appropriately.

16. DHS Furnished Facilities, Supplies and Services (<<Completed by User>>)

If work at *DHS S&T or CISA* is necessary for the services being performed under this Task Order, such facilities will be provided at offices at the appropriate location Parking facilities are not provided. Basic facilities such as workspace and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable and general-purpose office supplies) will be provided to HSOAC personnel.

DHS Furnished Property – a quarterly report of all S&T property should be submitted to the COR |HSOAC of all equipment purchased on behalf of the Government, and Government Furnished equipment being utilized by either HSOAC.

Subsequently a yearly report of all Government Furnished Equipment shall be provided to the COR | HSOAC. The COR | HSOAC will need a property form filled out for all S&T Contractor Acquired Equipment /Property or purchases on behalf of the Government for insertion into the S&T property management system (SAMS). This insertion will need to include the property form filled out in its entirety, paid invoice(s) showing the property purchase and a picture of the current state of that property.

a) Additional DHS property will not be provided to the HSOAC unless otherwise agreed. If DHS property is provided to the HSOAC for task performance, the HSOAC shall maintain property records, sending a yearly report of all items currently attached to the task order to the COR|HSOAC and the Program Manager and a disposition of the property must be completed at the end of the period of performance.
b) Before purchasing any individual item equal to or exceeding $5,000 that is required to support technical tasks performed pursuant to this Task Order, that has not already been accepted by the Government with the issuance of the Task Order, the HSOAC shall obtain prior written consent from the Program Manager, DHS IDIQ Contracting Officer, and DHS IDIQ COR. The HSOAC shall maintain any such items according to the IDIQ Contract's property accountability procedures, and FAR Part 45.
c) All DHS/GFP/GFE (IT equipment, building passes etc.) must be returned at the conclusion of the task order in accordance with component's procedures.
d) If any GFP/GFE is not returned, a report of survey must be submitted to the COR and Project Manager, referencing the DHS equipment number, pass or card number, name of individual to whom equipment was issued, and the last known location of property. Contractors who lose a badge will be required to fill out an additional lost badge form.

17. DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS 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 Enterprise Data Management Office (EDMO) 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 all data-related artifacts will be developed and validated according to DHS 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.

18. 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.

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

The offeror shall comply with the most current version of the DHS Cybersecurity Supply Chain Risk Management terms and conditions. (If the DHS C-SCRM T&Cs reference is not publicly accessible then the most current language will be added to this section of the TEP by the contracting officer prior to solicitation release)

20. Section 508 Requirements

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

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

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

20.1 1.1 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.

20.2 1.2 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

21. OCIO CISO Cyber-Supply Chain Risk Management (C-SCRM)

a. The Offeror understands and agrees that the Government retains the right to cancel or terminate the Contract, if the Government determines that continuing this solicitation presents an unacceptable risk to national security.

b. "Gray-Market" Equipment

    i. The Offeror shall provide only new equipment unless otherwise expressly approved, in writing, by the DHS Contracting Officer. Offerors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

    ii. The Offeror shall be excused from using new OEM (i.e., "gray market", "previously used") components only with formal Government approval, in writing, from the DHS Contracting Officer. Such components shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

    iii. All equipment obtained by the Offeror on behalf of the Government will need to be provided to OIG OCIO for review to validate requirements and approved Contractors by DHS.

c. Hardware and Software Requests

i. The contractors supply the Government hardware and software will provide the manufacturer's name, address, state, and/or domain of registration, and the DUNS number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNS number of those suppliers must be provided.

ii. Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors will perform due diligence to ensure that these standards are met.

iii. The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

1. For software products, the Offeror shall provide all OEM software updates to correct defects for the life of the product (i.e., until the "End of Life (EoL)"). Software updates and patches shall be either: made available to the government for all products procured under this Contract, replaced upon End of Support (EoS) is reached, or formally waived (in writing) by the DHS Contracting Officer.

d. Supply-Chain Transport

i. Offerors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill Contract obligations with the Government.

ii. All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the Contract, the period of performance, or one calendar year from the date the activity occurred.

iii. This transit process shall minimize the number of times in route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

iv. All records pertaining to the transit, storage, and delivery shall be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

v. The Offeror is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the

Government.

vi. The Offeror shall provide a packing slip which shall accompany each container or package with the information identifying this solicitation number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

vii. The Offeror shall send a shipping notification to the intended government recipient; with a copy transmitted via email to the Contracting Officer, or designated representative. This shipping notification shall be sent electronically and will state this solicitation number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Notifications

i. The Offeror shall notify DHS Contracting Officer, COR and the Office of the Chief Information Officer and the DHS component Chief Information Officer through the Enterprise Security Operations Center (ESOC) directly of any suspected or potential violations of Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT) at NDAA_Incidents@hq.dhs.gov.

f. Foreign Equities

The Offeror shall immediately notify the DHS Contracting Officer, COR that will report to the Office of the Chief Security Officer (OCSO) or cognizant component personnel security office regarding any changes to corporate foreign ownership, control, or influence.

22. Invoices

HSOAC will submit invoices on the 20th of each month. If the 20th of a month is a weekend or federally recognized holiday, the invoice shall be submitted on the first operating business day thereafter. Invoices should be submitted to the following accounts: [redacted]

23. Points of Contact

Government POCs	**Corresponding HSOAC POCs**
Program Manager	**HSOAC Task Lead**

[redacted] Program Manager DHS S&T/MCS [redacted]	[redacted] The RAND Corporation [redacted]
Contracting Officer's Representative [redacted] FFRDC PMO Deputy Director and COR DHS S&T/OIC/FFRDC [redacted]	**HSOAC Program Director/Portfolio Manager** [redacted] Director, Management, Technology & Capabilities Program Homeland Security Research Division The RAND Corporation [redacted]
Contract Officer [redacted] Contracting Officer DHS/MGMT/OPO [redacted]	**HSOAC Operations and Contracts Leads** [redacted] Director of Operations Homeland Security Research Division The RAND Corporation [redacted] [redacted] HSOAC Contract Administrator The RAND Corporation [redacted]
Suitability/Fitness Point of Contact [redacted] Security Specialist DHS S&T\OES\ASD\SPCO [redacted]	**HSOAC Security Staff** [redacted]

Additional Points of Contact (Optional)	**Notes: CISA POC for Task**
Alternate (PM), Technical Point of Contact (TPOC) [redacted]	

Program Manager – Product & Training CISA School Safety Task Force [redacted]	