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

U.S. Department of Homeland Security

Title: Understanding and Improving the Effectiveness of DHS Emergency Management Communications

Directorate/Division: Science and Technology Directorate (S&T)
FFRDC: Homeland Security Operational Analysis Center (HSOAC)

Version: 1.0

Date: April 18, 2024

1. Challenge

Emergency management communication for mitigation, preparedness, response and recovery aligns with DHS Mission 5, Build a Resilient Nation and Respond to Incidents. The DHS Quadrennial Homeland Security Review, issued April 2023, calls for the improvement of the institutional capacity that includes enhanced external affairs and strategic communications functions.[1] A comprehensive understanding of current DHS emergency management communication processes, threats to effective communications, and candidate approaches for mitigating and preparing for the threats will inform capacity building, programming, and research for more resilient incident response and recovery.

2. Outcome(s)

The primary outcomes of this study will be an improved understanding of barriers to emergency management communications, the risks to resilience caused by these barriers, and candidate approaches for reducing the risks. Beneficiaries of the S&T activities are likely to include multiple components across DHS (e.g. S&T Community and Infrastructure Resilience Program, Federal Emergency Management Administration (FEMA), Office of Health Security, Center for Prevention Programs and Partnerships [PLCY/CP3]) other emergency management agencies across the federal government (CDC, DHHS) and State, Local, Tribal and Territorial governments (SLTT).

[1] The Third Quadrennial Homeland Security Review (dhs.gov), p56.

3. Background

Effective emergency management communications are essential for mitigation, preparedness, and incident response and recovery.[2,3] External factors can reduce the fidelity of emergency management communications by decaying trust in the response plans.[4,5,6,7] The need to more precisely understand and counter barriers/threats to effective emergency management communications is a priority for DHS.[8]

Previous research has demonstrated that overall trust in government institutions has declined over time and differently across subpopulations (e.g., gender, age, education).[9] The decline has hindered the effectiveness of emergency management communications by changing the public perception of risk, reducing the clarity of communications, reducing the willingness to comply and generally decreasing the integrity of governmental organizations .[10,11] This relationship is increasingly pernicious as new communication technologies become more accessible.[12,13] The decay has impacted emergency management communications at multiple levels: within agency, interagency, agency to public, and with elected officials.[14,15]

S&T has asked HSOAC to examine current and potential emergency management communications through a detailed assessment of current programs for different phases of emergency management (i.e., mitigation, preparedness, crisis/response, recovery/restoration), development of a landscape analysis, a research agenda to guide programming, and a toolkit that DHS personnel can use to assist their emergency management communications efforts. This work aligns with the 4 objectives under *Mission 5: Build a Resilient Nation and Respond to Incidents*:

---

[2] National Incident Management System (fema.gov)

[3] Community and Individual Disaster Resilience for Floods: Options for Improving Protective Action Guidance | RAND

[4] Online posts spread misinformation about FEMA aid following Maui wildfires | AP News

[5] Countering False Information on Social Media in Disasters and Emergencies, March 2018 (dhs.gov)

[6] Beware of Misinformation/ Disinformation and Individuals and Businesses Posing as Claims Office Representatives | FEMA.gov

[7] Coronavirus Rumor Control | FEMA.gov

[8] https://www.domesticpreparedness.com/articles/a-foreign-government-oprah-and-fires-in-maui

[9] The Drivers of Institutional Trust and Distrust: Exploring Components of Trustworthiness | RAND

[10] Learning from COVID-19: government leaders' perspectives to improve emergency risk communication (biomedcentral.com)

[11] CSI-DEEPFAKE-THREATS.PDF (defense.gov)

[12] (PDF) The Emergence of Deepfake Technology: A Review (researchgate.net)

[13] Effect of Artificial Intelligence on Social Trust in American Institutions | TUP Journals & Magazine | IEEE Xplore

[14] Truth Decay and National Security: Intersections, Insights, and Questions for Future Research | RAND

[15] Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life | RAND

- 5.1 – Coordinate Federal Response to Incidents
- 5.2 – Strengthen the Security and Resilience of Critical Infrastructure
- 5.3 – Support Equitable Community Recovery
- 5.4 – Enhance Training and Readiness of First Responders.

This work also aligns with the three focus areas of the Social Science Technology Centers in S&T:

- Focus Area 1: Motivations and Drivers – This focus area aims to increase our understanding of the underlying motivations and drivers of specific human-centric DHS missions and produce the knowledge, fundamental understanding, and tools necessary to manage risk, find remedies for ills, and prepare for change in the future of DHS missions.
- Focus Area 2: Changing Behavioral and Social Implications – This focus area aims to improve our awareness and understanding of how changes in the technology landscape (particularly as science and technology continues to evolve) impact social interactions, behaviors, and threat vectors.
- Focus Area 3: Technology Acceptance and Limitations – This focus area aims to advance the acceptance of new technologies into DHS missions.[16]

4. Task Objective(s)

To assist DHS in achieving the stated outcomes of this task, HSOAC will conduct a review of the current DHS emergency management communications programs, policies, practices, and performance for different phases of emergency management (i.e., for different phases of emergency management (i.e., mitigation, preparedness, crisis/response, recovery/restoration), and the research requirements to strengthen those measures. Based on this assessment HSOAC will develop a landscape analysis, a research agenda to identify research requirements that S&T could address to mitigate component vulnerabilities, and a toolkit to assist response/recovery communities and the components with integrating S&T guidance into their emergency management communications systems. Together these analyses will provide the foundation for scientific understanding that can be used to develop a research program and guide efforts to improve emergency management communications among the DHS components.

5. Technical Approach / Analytic Methodology

Identifying, more precisely understanding, and countering the external barriers to effective emergency management communications has emerged as a pressing challenge to the United States Government. While various government agencies have tackled the barriers in many ways, a critical next step is to develop knowledge that will inform a comprehensive and science-based strategy for engagement with these barriers. The goal of this project is to collect information about DHS emergency management communications programs, identify barriers, and develop a multi-pronged research strategy to more precisely understand and share

[16] Technology Centers Research Agenda (dhs.gov)

methods to bypass the barriers. This review will be multi-disciplinary, including disciplines such as sociology, criminology, communications, business, marketing (e.g., FEMA sponsored marketing assessment), and political science.

Task 1, Review DHS Emergency Management Communications Procedures

HSOAC will conduct a systematic review of existing DHS emergency management communications procedures (i.e., programming, plans, policies) to identify potential facilitators and barriers to effectiveness across levels of the socioecological model (SEM). The SEM '...considers the complex interplay between individual, relationship, community, and societal factors. It allows us to understand the range of factors that put people at risk....'[17] The review will include a detailed analysis of emergency management communications challenges for achieving the objectives of *Mission 5: Build a Resilient Nation and Respond to Incidents* from the Quarterly Homeland Security Review 2023 and related DHS documents. HSOAC will select 2-3 components within DHS to review their standard communications procedures and compare them to their emergency management communications procedures in 2-3 selected emergency types (e.g., pandemic, natural disaster). This effort will be summarized in a landscape analysis that will identify gaps in the procedures, programming, plans and policies and provide recommendations for resolving the gaps.

HSOAC will engage the emergency response/recovery community in this process through an outreach and advisory panel (OAP). HSOAC will convene a panel of experts from USG and peer-equivalent agency representatives with expertise in emergency management communications. The OAP will not reach a group consensus on any topics. HSOAC will capture recommendations from the group of experts and subsequently provide their own independent assessment of DHS emergency management communications procedures. Experts may include members of the International Association of Chiefs of Police Public Information Officers Section, businesses that provide emergency management communications services for police/fire/EMS and state or local government agencies, Association of Public Safety Communications Officials (APCO), and the National Interagency Fire Center. Panel members will be paid consultants and will provide input for the landscape analysis and toolkit to further refine the deliverables.

Task 2, Conduct Literature Review

HSOAC will review the current published research evidence about effective emergency management communications, including facilitators and barriers/threats to effectiveness across the SEM. The review will include an in-depth examination of the relationship between institutional trust and the effectiveness of official emergency management communications. The review will be used to identify studies that may address the gaps from Task 1 and will be presented in the research agenda reports.

Specific topics will be selected based on Task 1 and may include:

- Emergency management communications to the public – overview.
- Emergency management communications to the emergency services sector – overview.

[17] The Social-Ecological Model: A Framework for Prevention | Violence Prevention | Injury Center | CDC

- Emergency management communications to affected critical infrastructure providers – overview.
- Performance metrics for effective emergency management communications (e.g., correctness, completeness, timeliness, robustness, understandability/accessibility, believability/credibility, impact, coordinated messaging among federal emergency service providers (such as DHS, CDC)) to the public, to the emergency services sector, and to affected critical infrastructure providers.
- Critical elements of institutional trust, including public trust in official communications and federal agencies, during different phases of emergency management (mitigation, preparedness activities, crisis/response, recovery/restoration).
- Performance metrics for institutional trust and distrust and public awareness and response to official communications
- Facilitators to effective communications about emergency events during different phases of emergency management (mitigation, preparedness activities, crisis/response, recovery/restoration)
- Barriers/threats to effective communications about emergency events during different phases of emergency management (mitigation, preparedness activities, crisis/response, recovery/restoration)
- Methods to improve effectiveness of emergency management communications (e.g., correctness, completeness, timeliness, robustness, understandability/accessibility, believability/credibility, impact, coordinated messaging among federal emergency service providers (such as DHS, CDC)), including methods to build the institutional trust needed for effective emergency management communications, especially in the presence of identified barriers/threats.

Task 3, Document Findings and Develop Recommendations. HSOAC will provide the following deliverables:

- **A. Landscape Analysis, of DHS Emergency Management Communications.** Using the results from Tasks 1 and 2, HSOAC will summarize the current emergency management communications landscape at DHS. HSOAC will conduct a landscape analysis summarizing current emergency communications practices, threats, and opportunities. HSOAC will use the landscape analysis to develop the research agendas and educational toolkit described below. The landscape analysis will be presented in a briefing to DHS S&T.

- **B. Research Agenda, Critical Barriers to Effective Emergency Management Communications.** HSOAC will draw on Tasks 1 and 2 to describe barriers to effectiveness of emergency management communications across levels of the socioecological model (SEM). The assessment will include short summaries of especially critical barriers, including targeted review of relevant DHS policies and recommendations for further research to more precisely understand and address critical

barriers. HSOAC will prioritize the topics into a recommended research agenda based on alignment with the communication needs identified by the QHSR review in Task 1. The critical barriers research agenda will be presented in a briefing to DHS S&T.

- **C. Research Agenda, Institutional Trust and Official Communications**. HSOAC will draw on Tasks 1 and 2 to review the relationship between public trust in institutions and the effectiveness of official communications across levels of the socioecological model (SEM) and during different phases of emergency management (mitigation, preparedness activities, crisis/response, recovery/restoration). HSOAC will prioritize the topics into a recommended research agenda based on alignment with the communication needs identified by the QHSR review in Task 1. The institutional trust and official communications research agenda will be presented in a briefing to DHS S&T.

- **D. Research Report, Landscape Analysis of DHS Emergency Management Communications and Foundational Research Priorities**. HSOAC will draw on Tasks 1 and 2 to produce a publicly available research report.

- **E. Toolkit, for DHS Emergency Management Communications**. Using the results from Tasks 1 and 2, HSOAC will identify top recommendations for improvements to emergency communications that DHS personnel can make today, including both to-dos and don't dos. These will cover top strategies and tips for communications strategies (focusing on trust-building mechanisms), performance measurement, and approaches for addressing specific barriers to effective communication, as known. These will be captured in a toolkit – a set of easy-to-use quick-guides, checklists (and other templates, as appropriate), and reference white papers that DHS personnel can use to assist their emergency communications efforts.

Data Management

HSOAC may collect and use PII in the form of business contact information from stakeholders to conduct workshops and in-person meetings. CUI will be stored and remain in the HSOAC IT Enclave.

HSOAC will require recurring access to government facilities. HSOAC will retain CUI in accordance with the applicable records schedule. To support the long-term needs of the Department as its federally funded research and development center (FFRDC) for studies and analysis, HSOAC will retain the data over the period of performance of the HSOAC FFRDC contract including follow-on contracts. Per PIA-042 FFRDC, PII is returned at the conclusion of the project to the providing DHS component, through secure methods, or destroyed. Some routine, non-sensitive business contact PII (e.g., names, email addresses) or enduring value to FFRDC projects may be retained; otherwise, business contact information contained in dedicated project files will be deleted when determined to be unnecessary.

6. Key Words

Type of Work

Emergency management communications analysis, social-ecological models, model, critical infrastructure preparedness. Landscape, research agenda, toolkit.

Benefit of Work

Improve critical infrastructure mitigation, preparedness, response, and recovery through improved communications.

Subject of Interest

Emergency management communications

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.

FFRDC proposed total STE: 0.68

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

At the intersection of the appropriate Focus Area row and QHSR Mission column, enter a percentage of the total STE. **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	0%	0%	0%	0%	100%	0%
3: Innovation and Technology Acceleration	0%	0%	0%	0%	0%	0%
4: Homeland Security Threat and Opportunity Studies	0%	0%	0%	0%	0%	0%
5: Personnel Policy and Management Studies	0%	0%	0%	0%	0%	0%
6: Operational Studies	0%	0%	0%	0%	0%	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 FFRDC 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 COR.

Table 2: Deliverables

Scope Ref.	Deliverable Name	Delivery Date
5.1-5.3	Project Management Plan (PMP) (Draft) <<Note IDIQ Requirement>>	15 days after award
5.1-5.3	Project Management Plan (PMP) (Final) <<Note IDIQ Requirement>>	30 days after award
5.1-5.3	Task Order Project Kickoff Briefing <<Note IDIQ Requirement>>	Within 30 days of project award date
5.1-5.3	Briefings/Meetings/IPRs	Kickoff briefing within 1 month of award. Regular meetings/IPRs (quarterly or ad hoc per sponsor needs)
5.3.A	Final Landscape Analysis –DHS Emergency Management Communications (S&T briefing)	5 months after award
5.3.B	Final Research Agenda – Critical Barriers to Effective Emergency Management Communications (S&T briefing)	9 months after award
5.3.C	Final - Research Agenda – Institutional Trust and Official Communications (S&T briefing)	13 months after award
5.3.D	Draft Research Report –DHS Emergency Management Communications and Foundational Research Priorities	13 months after award
5.3.E	Draft Toolkit	14 months after award
5.3.E	Final Toolkit	16 months after award
5.3.D	Final Research Report (publicly releasable RAND Research Report) –DHS Emergency Management Communications and Foundational Research Priorities	15 months after award

All	Final Task Completion Memo – Final documentation of deliverables and summary of work performed since final report delivered.	End of period of performance

The FFRDC shall provide all deliverables under this task order directly to the S&T FFRDC PMO (via hsoac.deliverables@hq.dhs.gov), the Task Order PM, TPOC, 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 FFRDC 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 FFRDC 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

N/A

10. Travel

Travel may be necessary to meet and coordinate interagency exchanges of information and to collect data for this task. The FFRDC 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
Washington D.C.	New York, NY	2	5
Washington D.C.	New York, NY	1	5
Boston, MA	New York, NY	1	5

- Total Number of Trips (All Travelers): 4
- Total Number of Travel Days (All Travelers): 20

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 18 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 ordering end date, 3/23/2027.

12. Security Requirements.

This Task Order will require access to the following information

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

12.1 Security requirement #2 (SBU, FOUO) – All unclassified "For Official Use Only" (FOUO) work is expected to occur at the "medium" level per the National Institute of Standards and Technology (NIST) 800-60 (Federal Information Processing Standard (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.

12.2 Security requirement # 2 (SBU, FOUO) – The Contractor shall safeguard SBU, FOUO information in accordance with DHS Management Directive 11042.1 and in compliance with all applicable terms and conditions of the contract, including HSAR Class Deviation 15-01 Safeguarding of Sensitive Information. The parties acknowledge that in order to align with current DHS acquisition policy the July 2023 HSAR Class Deviation 15-01, Revision 1 Safeguarding of Controlled Unclassified Information (CUI) clauses are expected to be incorporated via modification to this task order. The parties further acknowledge that any CUI handled, stored or in any way used in the performance of this task order prior to such modification will be safeguarded in the manner applicable to SBU and FOUO information.

12.3 The contractor shall use government accredited IT systems to accomplish this work, when applicable. Sensitive work is generally stored and processed within the HSOAC IT Enclave, or as otherwise noted in the Authorized IT Environment(s) and Data Overview (AIEDO). If classified work is required under this Task Order, the Task Order COR shall provide specific guidance to the FFRDC as to which work will be conducted in a classified manner and at which classification level. Classified information shall be stored and/or processed at the locations identified below under "Safeguarding/Storage" and as identified in the IDIQ DD 254 or subsequently issued task order DD 254. If such DHS-guidance conflicts with other applicable guidelines (e.g., DOE, DOD, etc.), the FFRDC shall adhere to the more stringent guidelines as determined by the Task Order COR and DHS FFRDC PMO. The FFRDC shall also adhere to other applicable government orders, guides, and directives pertaining to classified or confidential work.

12.4 Authorized IT Environments

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

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

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

12.5 DHS Furnished Information

a) DHS will provide unique information, materials, and forms to the Contractor as specified under this task order. Such DHS provided information, materials, and forms shall remain the property of DHS, unless otherwise indicated in writing by DHS, and may not be distributed beyond the FFRDC's project performers without DHS's prior written permission.
b) The DHS COR identified in this task order will be the point of contact (POC) for identifying required information to be supplied by DHS.

12.6 FFRDC Furnished Information

None

12.7 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 FFRDC.

14. Other Contract Details

In accordance with the language in the FFRDC 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 FFRDC Personnel

Personnel provided by the FFRDC will have the skills and technical background necessary to successfully complete the tasks described in this plan. The FFRDC 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 FFRDC 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 FFRDC'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 FFRDC.

The FFRDC 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 FFRDC 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 FFRDC 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 FFRDC 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 FFRDC 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 FFRDC 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 FFRDC 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), FFRDC 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 FFRDC 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 FFRDC 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 FFRDC 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 FFRDC 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 FFRDC 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 FFRDC COR. Seminars, workshops, and short-courses intended to extend the access and awareness of FFRDC 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 FFRDC 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 FFRDC 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 FFRDC or FFRDC operator in anyway. The FFRDC therefore will generally seek public release approval for the results of non-sensitive research. Thirty (30) days prior to release, the FFRDC will first ask for the task order COR's and CO's agreement that the research product is suitable for release. The FFRDC 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 FFRDC's analytical conclusions, final findings, or analytical outcomes.

As outlined in this TEP and the IDIQ contract, the sponsor is interested in widespread dissemination of the results of funded non-sensitive research so that the sponsor, other DHS Components, and DHS partners can gain benefit from these results now and in the future. As mentioned in response to the questions that follow, the sponsor will work with HSOAC to develop an appropriate dissemination strategy for sharing project results that will support accomplishment of the objectives outlined in this TEP. This plan will include public release of an HSOAC report that documents results of this study that are not DHS Sensitive.

Similarly, to increase the benefits of this study for DHS partners, HSOAC will work with the sponsor to share results that are DHS Sensitive with appropriate audiences using appropriate means that assure need-to-know and authority to access information at the specified sensitivity.

- 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, other DHS officials, DHS partners in accomplishing the missions addressed by the study, and other research organizations contributing to supporting DHS in these mission areas. 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.

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

If work at *DHS S&T* 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 work space and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable and general purpose office supplies) will be provided to FFRDC personnel.

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

Subsequently a yearly report of all Government Furnished Equipment shall be provided to the COR | FFRDC. The COR | FFRDC 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 FFRDC unless otherwise agreed. If DHS property is provided to the FFRDC for task performance, the FFRDC shall maintain property records, sending a yearly report of all items currently attached to the task order to the COR|FFRDC 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 FFRDC shall obtain prior written consent from the Program Manager, DHS IDIQ Contracting Officer, and DHS IDIQ COR. The FFRDC 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. Invoices

HSOAC invoices will generally be sent on or soon after the 20th of each month to the PM, COR, CO, ffrdc.invoices@hq.dhs.gov and invoicesat.consolidation@ice.dhs.gov.

18. Points of Contact

Government POCs	Corresponding FFRDC POCs

Program Manager [redacted] Social Science SME DHS S&T [redacted]	**FFRDC Task Lead** [redacted] Senior Political Scientist HSOAC [redacted]
Contracting Officer's Representative [redacted] Business Operations Manager FFRDC PMO [redacted]	**FFRDC Program Director/Portfolio Manager** [redacted] Director, Disaster Management & Resilience Program, HSOAC Homeland Security Research Division The RAND Corporation [redacted]
Contract Officer [redacted] Contracting Officer DHS/MGMT/OPO [redacted]	**FFRDC Contracts Leads** [redacted] HSOAC Contract Administrator The RAND Corporation [redacted]
Suitability/Fitness Point of Contact [redacted] Security Specialist DHS S&T\OES\ASD\SPCO [redacted]	**FFRDC Security Staff** [redacted]