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

U.S. Department of Homeland Security

Title: Emerging Technology and Risk Analysis

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

Version: 1.0

Date: July 19, 2022

1. Challenge

The Office of Strategy, Policy, and Plans (PLCY) has come forward with a requirement to continue the basic research and analysis of DHS Emerging Technologies previously performed by S&T in support of the PLCY R2PC. In the previous effort, a considerable number of possible emerging risks were identified, and a number of DHS Components and outside entities were asked to rank the risks. The final product of the survey was an infographic, mapping the results of components and outside entities and presenting a concise list of new and evolving risks, documented above. The process was a single, manual effort to survey and rank the risks and provided no further output. In order to take tangible steps towards closing or mitigating these risks, the risks must be further defined and understood. The required analyses will provide better context to these risks, informing how and when they could impact the Nation and the Department, which then enables the Department to plan resources, programs, strategy, and policy to address the risks in a timely manner.

Recurring risk assessments are essential to informing near and long-term policy development and investments. Currently, there are no programmed, recurring risk assessments that cover the range of current and potential future DHS mission activities across specific technologies.

2. Outcome(s)

This research will inform senior DHS decisionmakers on emerging technology risks and the R&D and policy opportunities to mitigate the impact of these risks on DHS missions. Ultimately this effort will allow S&T and PLCY to have a better understanding and analysis of the risk(s) and

their impacts in order to inform potential new guidance, strategy, investments and/or policy that may be necessary to address and/or mitigate specific risks from emerging technologies.

3. Background

Threats: DHS has conducted a lot of work understanding the threat and hazard landscape. For instance, in 2016, the **DHS Office of Policy (PLCY)** identified and characterized 28 threats and hazards that represented the "greatest homeland security risks to the nation".[1] As described in a forthcoming HSOAC publication, "these threats and hazards have the potential for a significant national impact on health, safety, security, the economy, the natural environment, or the continuity of governance—or some combination of these".[2] Similarly, I&A continually creates and documents threat scenarios which identify potential harms to the homeland. Many of these threats pose the potential for use of technologies, by either the threat actor or the defender.

Technologies: Next, consider the technologies. **S&T's** mission is to "enable effective, efficient, and secure operations across all homeland security missions by applying scientific, engineering, analytic, and innovative approaches to deliver timely solutions and support departmental acquisitions." Part of this mission is to mature and strengthen the Homeland Security Enterprise (HSE) through the development of scientifically and technically-sound recommendations for science policy and strategy at the Department level. Another part of that mission is to understand current S&T investments and make recommendations on R&D and acquisition programs to fill capability gaps moving forward. As a result of these missions, S&T works to assist Components in fielding technology as efficiently and innovatively as possible. For example, the focus of the S&T MCS "Checked Baggage" program considers a variety of scanning, chemical detection, and artificial intelligence/machine learning technologies. Other programs might require advanced technologies for training law enforcement officers, or technologies to understand where first responders are in a building, or technologies to ingest social media and predict potential violent extremism events. In addition, there are other parts of S&T (such as the Office of SAFETY Act Implementation [OSAI]) that maintain, for example, lists of Qualified Anti-Terrorism Technologies. Given this, S&T's focus will be on set of emerging technologies, earlier identified and prioritized by R2PC :

- Countering cyber operations (i.e., physical)
- Countering cyber operations (i.e., virtual)
- Countering information and influence operations
- Biological agent and weapon advance detection

---

[1] This resulted in the 2018 Homeland Security National Risk Characterization

[2] See Stapleton et al., "Harnessing the Power of Science and Technology Communities for Crisis Response," 2022, forthcoming.

- Unmanned vehicles (e.g., piloted, augmented, autonomous) melding emerging technologies
- Synthetic content (e.g., deep fakes, voices, personalization, smart chatbots)
- Additive manufacturing
- Learning systems (i.e., includes machine learning and deep learning)
- Leading next generation communications protocols (i.e., 6G, nG)
- Intelligent UxS swarms

As DHS begins planning for risk assessment of emerging technologies for PLCY, along with accompanying policy and guidance to act quickly in the face of a new threat or to begin the planning and coordination activities for known threats, there needs to be an understanding of the technology landscape for the next 2-5 years. HSOAC has experience in understanding current and emerging technology needs across existing MCS portfolios,[3] as well as conducting technology landscape assessments (such as mitigating risks posed by the microelectronics supply chain[4]), or working with DHS stakeholders to address the risks posed by cyber supply chains.[5] HSOAC also worked with the predecessor DHS S&T Emerging Technologies and Risks Program to provide input to PLCY in 2019. HSOAC can leverage the data collected for that effort as a starting point for some of the analysis identified below.

4. Task Objective(s)

HSOAC will work with S&T to conduct an analysis on identified emerging technologies to develop 2-4 page white papers addressing the below items:

1) Detailed description of the technology
    i. Benefits or opportunities afforded by technology
    ii. Harms or threats afforded by the technology to both the DHS Mission and the Nation
    iii. Missions and Components potentially impacted by the technology

---

[3] See unpublished technology roadmap for Electronic Baggage Screening Protocol, as well as the related publicly available perspective, Airline Security Through Artificial Intelligence: How the Transportation Security Administration Can Use Machine Learning to Improve the Electronic Baggage Screening Program | RAND ; https://www.rand.org/pubs/perspectives/PEA731-1.html

[4] O'Connell et al. Managing Risk in Globalized Supply Chains. RR-A425-1, 2021.; Gonzales et al. Unclassified and Secure: A Defense Industrial Base Cyber Protection Program for Unclassified Defense Networks. RR-4227-RC, 2020.; Slomovic, A. An Analysis of Military and Commercial Microelectronics: Has DoD's R&D Funding Had the Desired Effect? N-3318-RGSD, 1991.; Slomovic, A. Anteing Up: The Government's Role in the Microelectronics Industry. P-7516-RGS, 1988.

[5] Bonds et al. America's 5G Era: Gaining Competitive Advantages While Securing the Country and Its People. PE-A435-1, 2021.

2) Likelihood of emergence (i.e., for near-, mid-, and long-term)
    i. Maturity of the technology
    ii. Contributing factors (e.g., policy, technical, etc.)
    iii. Critical events or converging technologies
        a. Timelines and confidence of assessments
        b. Scope of potential impact and confidence of assessments
    iv. Size/scale of potential issue
    v. Current or planned capabilities
    vi. Necessary capabilities

Here, near- term is defined as up to 3 years, mid- term is defined as 3-5 years, and long-term is defined as 5-10 years.

5. Technical Approach / Analytic Methodology

To achieve the outcomes and objectives presented, HSOAC proposes the following tasks.

Task 1: Develop Impact Framework and Metrics: HSOAC will develop, independent of threats and technologies, an S&T-wide impact framework and set associated of metrics (across output, outcome, and long-term impact) applicable to Task 2 and the Optional Tasks (white papers). The framework will allow for comparability of white paper impact across different technologies, ranging across physical (e.g., drones, chemical scanning, 6G, satellite), computer (e.g., artificial intelligence, machine learning), and others (advanced applications of social science). This could, for example, consider the Qualified Anti-Terrorism Technologies under the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act.[6] The white paper metrics will include a range of output, outcome, and long-term impacts that might be used to convey the value of the work to stakeholders. For example, white paper metrics might include a) number of Components impacted, b) number of policy recommendations anticipated, c) or anticipated funding provided to follow up technology characterization, assessment, prototyping, or potential exploitation which is acted upon by S&T, HQ, or other DHS Components. This framework will be constructed to ultimately allow the user to standardize / characterize recommended actions for traceability and measurement of the impact of the white paper after the fact.

HSOAC will document the data sources, method(s) of analysis, and findings in Interim Progress Review (powerpoint briefing). This will occur at approximately 2 months after task award.

[6] See documentation at DHS SAFETY Act (Home) ; https://www.safetyact.gov/

Task 2: White Paper on Topic 1. After the sponsor and HSOAC agree on the first topic, HSOAC will develop a 2-4 page white paper (with supporting documentation in the appendix) addressing the below items:

3) Detailed description of the technology
    i. Benefits or opportunities afforded by technology
    ii. Harms or threats afforded by the technology to both the DHS Mission and the Nation
    iii. Missions and Components potentially impacted by the technology
4) Likelihood of emergence (i.e., for near-, mid-, and long-term)
    i. Maturity of the technology
    ii. Contributing factors (e.g., policy, technical, etc.)
    iii. Critical events or converging technologies
        a. Timelines and confidence of assessments
        b. Scope of potential impact and confidence of assessments
    iv. Size/scale of potential issue
    v. Current or planned capabilities
    vi. Necessary capabilities

At approximately 15-20% of completion, the initial scoping will be presented as an interim progress report. The IPR will include in attendance the performer (HSOAC) and the sponsor's invitees of technical subject matter experts (SMEs) and stakeholders. The attendees will have two weeks to provide comments on the framework product. After comment, HSOAC will provide a draft report for sponsor review, and upon receipt of sponsor comments, HSOAC will provide a final report.

HSOAC will also provide an executive briefing or infographic (no higher classification than FOUO data) on the outcome of the analysis, highlighting key technologies and recommendations.

(Option 1-9) Task 3: Conduct Remaining Deep-dive Research in Identified Technologies. This Option may be enacted once for each of the nine remaining technologies.

For each Option enacted, HSOAC will write a 2-4 page white paper (with supporting documentation in the appendix) addressing the same topics as listed in Task 2. The analysis will be tailored to the technologies, and may include (for example) a description of the current technology readiness level, characteristics of the technology relevant to the threat scenarios (which may vary widely across hardware and software applications), a list of open research topics for this technology that will likely need addressed prior to achieving a technology readiness level of 9, potential follow-on for R&D, and relevant policy or strategy considerations for the Department.

For each time the Option is enacted, HSOAC will also provide an executive briefing or infographic (no higher classification than FOUO data) on the outcome of the analysis, highlighting key technologies and recommendations.

6. Key Words

Type of Work

Technology Roadmapping, threat analysis, expert elicitation, decision analysis

Benefit of Work

inform senior DHS decisionmakers on emerging technology risks, improve R&D coordination, improve R&D investments, increase capability effectiveness, improve R&D transparency, improve policy, improve science-based decisionmaking

Subject of Interest

Counter unmanned aerial vehicle / systems (cUAV / cUAS), Artificial intelligence / machine learning (AI / ML), biometrics ((e.g., fingerprints, facial images, DNA, voice, iris), DNA rapid prototyping, Big data analytics, Surveys, Position, Navigation and Timing (PNT), National economic impact, Critical asset risk assessment, Social media or publicly available information, Advanced wireless services, Wireless Device Detection, Cybersecurity, 5G, hypersonics, R&D, acquisition, investments

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:__Base: 0.22; Options 1-3: 0.22; Options 4-8: 0.21; Option 9: 0.20____

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. << In this section, across all work to be performed, categorize the work against one or more FFRDC focus areas and QHSR mission areas. Note: because the FFRDCs have different focus areas, there are 2 tables. **Delete the table that does not apply.>>**

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%	0%	0%
3: Innovation and Technology Acceleration	50%	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 (R&D) Studies	0%	0%	0%	0%	0%	50%

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. The Contractor shall not use, release to others, reproduce, distribute, or publish any data first produced or specifically used in the performance of this Contract for its own private purposes without prior written approval from DHS pursuant to FAR Rights in Data – General (May 2014) 52.227-14(d)(2).

Table 2: Deliverables

Scope Ref.	Deliverable Name	Delivery Date

5.0.1	Project Management Plan (PMP) (Draft) <<Note IDIQ Requirement>>	15 days after award
5.0.2	Project Management Plan (PMP) (Final) <<Note IDIQ Requirement>>	30 days after award
5.0.3	Task Order Project Kickoff Briefing <<Note IDIQ Requirement>>	Within 20 days of project award date
5.1	Interim Progress Report 1: Framework & Metrics	2 months after award
5.2	Interim Progress Report 2: 15-20% review of Technology 1	9 weeks after award
5.3	Technology 1: Draft 2-4 page report	19 weeks after award
5.3	Technology 1: Final 2-4 page report and executive briefing	23 weeks after award
5.4	[Optional Tasks 1-9] For each option enacted, one 15-20% review of Technology 1	6 weeks after each optional award
5.4	[Optional Tasks 1-9] For each option enacted, one draft 2-4 page report	16 weeks after award
5.4	[Optional Tasks 1-9] For each option enacted, one final 2-4 page report and executive briefing	20 weeks after option award or End of optional award period of performance

The FFRDC shall provide all deliverables under this task order directly to the S&T FFRDC PMO (via [redacted], 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

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 FFRDC 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 FFRDC 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 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
PIT	DCA	2	2
LAX	DCA	2	3

- Total Number of Trips (All Travelers): 4
- Total Number of Travel Days (All Travelers): 10

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

Period of performance is two years. The deliverables for each optional task are due 6 months from the date the option is exercised. Optional tasks may be exercised starting two months into the PoP.

12. Security Requirements.

This Task Order will require access to the following information << DELETE NON-APPLICABLE BOXES – doing this streamlines Appendix G submissions >>:

- ☒ 1. Unclassified, no markings
- ☒ 2. Sensitive but Unclassified (SBU), For Official Use Only (FOUO)
- ☒ 3. Law Enforcement Sensitive (LES)
- ☐ 4. Personally Identifiable Information (PII)
- ☒ 5. Protected Critical Infrastructure Information (PCII)
- ☒ 6. Confidential (classified)
- ☒ 7. Secret (classified)
- ☒ 8. Top Secret (classified)
- ☒ 9. Top Secret/SCI (classified)
- ☐ 10. Fill in other classification(s) if needed, e.g., Sensitive Security Information (SSI), Secret National Security Information (SNSI), Chemical-terrorism Vulnerability Information (CVI)"

<< GOVERNMENT PM DELETE NON-APPLICABLE SUB-SECTIONS BELOW - doing this streamlines Appendix G submissions. >>

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 # 5 (PCII) – The FFRDC shall comply with all requirements of the Protected Critical Infrastructure Information (PCII) Program set out in the PCII Act, in the implementing regulations published in the Interim Rule, and in the PCII Procedures Manual as they may be amended from time to time, and shall safeguard PCII in accordance with the procedures contained therein.

12.3 Security requirement # 5 (PCII) – The FFRDC shall ensure that each of its employees, consultants, and subcontractors who work on the PCII Program have executed non-disclosure agreements (NDAs) in a form prescribed by the PCII Program Manager. The FFRDC shall ensure that each of its employees, consultants and subcontractors has executed an NDA and agrees that none of its employees, consultants or sub-contractors shall be given access to PCII without having previously executed a NDA.

12.4 Security requirement # 2 (SBU, FOUO) – The FFRDC shall adhere to all applicable government laws, regulations, orders, guides, and directives pertaining to classified, Sensitive But Unclassified (SBU), FOUO, or personally identifiable information. The contractor shall safeguard SBU, FOUO information specifically in accordance with DHS Management Directive 11042.1 and in compliance with HSAR Class Deviation 15-01 Safeguarding of Sensitive Information.

12.5 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 FFRDC 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 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.

12.6 Authorized IT Environments

<< Once authorized by DHS S&T, through issuance of an authority to operate (ATO), the FFRDC IT Enclave will be the primary environment for FFRDC project work for most all types of DHS Sensitive information. The Enclave will meet DHS 4300A Sensitive Systems standards. Note this section is not applicable to classified information, which is a separate category of information and the FFRDC Enclaves are NOT approved for classified information.>>

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).

12.7 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.

12.8 FFRDC Furnished Information

None.

12.9 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. SECRET level safeguarding/storage is needed at the FFRDC.

b. Classified work will be performed at the following location(s) :

Classified Work Locations

The RAND Corporation [redacted] Cage Code [redacted]	The RAND Corporation [redacted] Cage Code [redacted]

The RAND Corporation [redacted] Cage Code [redacted]	

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 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.

14.2 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.

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

For the TEP award, the sponsor is not interested in releasing information publicly from the research.

- If you don't want to release the results, is the FFRDC able to release info about the methodology to the other components or the public?
  While the methodology is not currently expected to be releasable, the sponsor is open to a discussion after the research is completed on whether they may be shareable with other components or the public.

- What is the desired audience for the release of info? Component only/all of DHS/public release?
  As outlined in this TEP, the audience is DHS PLY and S&T.

- Do you want an outreach event as part of the release?
  No.

- Would you be interested in having the PMO assist with the release of favorable results?
  Not applicable.

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

If work at *<< 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

Send invoices to the mailbox **S&T MCS Emerging Risks & Technologies** [redacted] by the 20th of each month.

COR: [redacted]

CO: [redacted]

HSOAC invoices will generally be sent on or soon after the 20th of each month.

18. Points of Contact

<< Note that if multiple offices/divisions contribute requirements to this task order, PM information is required for each. Insert alternates as necessary. >>

Government POCs	**Corresponding FFRDC POCs**
Program Manager [redacted] Program Manager S&T/ MCS [redacted]	**FFRDC Task Lead** [redacted] Research Engineer The RAND Corporation [redacted]
Contracting Officer's Representative	**FFRDC Program Director/Portfolio Manager**

[redacted] HSOAC Program Lead and COR FFRDC PMO/S&T [redacted]	[redacted] Director, Acquisition and Development Program, HSOAC Mathematician The RAND Corporation [redacted]
Contract Officer [redacted] Associate Director/Contracting Officer DHS/MGMT/CPO/OPO/S&TAD [redacted]	**FFRDC Operations and Contracts Leads** [redacted] HSOAC Director of Operations The RAND Corporation [redacted] [redacted] HSOAC Contract Administrator The RAND Corporation [redacted]
Suitability/Fitness Point of Contact [redacted] Security Specialist S&T/ASD/SEC [redacted]	**FFRDC Security Staff** [redacted]

<< Insert alternate POCs and add titles as necessary. >>

Additional Points of Contact (Optional)	**Notes:**
Alternate (PM, COR, etc.) Insert name Insert title Insert organization Insert phone number Insert email address	

Alternate (PM, COR, etc.) Insert name Insert title Insert organization Insert phone number Insert email address	