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

**U.S. Department of Homeland Security**

**Title: Balancing Business Risk Tolerance with National Security Risk**

**Component/Office: Office of the National Cyber Director (ONCD)**
**Directorate/Division: Executive Office of the President (EOP)**
**FFRDC: Homeland Security Operational Analysis Center (HSOAC)**

**Version: 1.0**

**Date:** August 20, 2024

## 1. Challenge

In executing its responsibility to promote practices enhancing the security of our digital ecosystem while preserving innovation, ONCD must better understand risk and risk tolerance, both in terms of theoretical frameworks to measure business risk and national security risk and how those frameworks should be applied within critical infrastructure sectors.

## 2. Outcome(s)

This study will inform the Office of the National Cyber Director (ONCD) on the ways to quantify national security risks – as opposed to business risks - within critical infrastructure sectors. It would identify and document various risk management frameworks used by federal agencies and critical infrastructure owners and operators to identify, manage, and reduce various risks, including disruption to services, economic losses, and national security impacts. It would also provide a national framework to help the government identify national security risks related to cyber incidents and consider mitigations that can help reduce those risks. Finally, the study would identify opportunities for the Federal government to incentivize implementation of cybersecurity practices to mitigate national security risks.

## 3. Background

The National Cyber Director (NCD) serves as the principal advisor to the President on cybersecurity policy and strategy relating to the coordination of programs and policies intended to improve the cybersecurity posture of the United States. In line with the 2023 National Cybersecurity Strategy, ONCD is responsible for shaping policy that promotes practices that enhance the security and resilience of our digital ecosystem while preserving innovation and competition.

In March 2024, the National Security Telecommunications Advisory Committee (NSTAC) released a report with the stated purpose of recommending "ways to incentivize cybersecurity best practices, reduce barriers to their implementation, and measure best-practice adoption." In crafting this report, the NSTAC sought consultation from subject matter experts to gain insight into the "challenges and experiences organizations encounter when implementing and assessing the effectiveness of cybersecurity programs." The NSTAC sought to assess the gap "what markets naturally provide and what national security and emergency preparedness require" in cybersecurity decision-making. In particular, the report found that there is a gap between funding needed to mitigate national security risk and the funding a business is willing to put toward cybersecurity to address risk realized by the business itself. The report also found

that "strengthening the nation's cybersecurity depends on the ability of public and private sector decision makers to make risk-informed decisions on the most effective solutions available when allocating limited resources." Finally, the report highlighted that greater support from the federal government is needed to support critical infrastructure owners and operators at risk "due to the ability of nation-state actors to intimidate, project power, and pre-position in case of future (or current) hostilities."

In executing its responsibility to promote practices enhancing the security of our digital ecosystem while preserving innovation, ONCD must better understand risk and risk tolerance, both in terms of theoretical frameworks to measure business risk and national security risk and how those frameworks should be applied within critical infrastructure sectors. Therefore, in support of the NCD's statutory mission and requirements in the National Cybersecurity Strategy, ONCD would benefit from this study utilizing the Department of Homeland Security (DHS) FFRDC operated by RAND. ONCD seeks to use this information to determine what cybersecurity practices should be incentivized through federal efforts to support mitigation of national security risk.

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Council (NSC), the National Economic Council (NEC), and the Department of Commerce (DOC) may also benefit from this analysis, and ONCD plans to consult with those agencies through the course of the study.

## 4. Task Objective(s)

The outcome of a successful partnership between ONCD and RAND Corporation (RAND) on the Balancing Business Risk Tolerance with National Security Risk project will be the analytical support, a discussion paper, a framework, and a case study to support ONCD's responsibilities to shape policies that preserve innovation and competition while improving resilience. RAND's primary responsibility will be the development of an analytical framework for understanding the differences in mitigations taken to address business risk and those taken to address a national security risk. RAND will provide a case study analysis to apply the framework to a critical infrastructure sector or subsector.

**The objectives of the task are**:

1. Identify and document various risk management frameworks used by federal agencies and critical infrastructure owners and operators to identify, manage, and reduce various risks, such as disruption to services, economic losses, and national security impacts;
2. Examine whether new or existing frameworks could be developed or modified to better treat business risks and social and national security risks as distinct factors for private entity decision makers, in order to better understand the range of potential outcomes associated with various policy tools aimed at incentivizing critical infrastructure operators to undertake desired risk mitigation investments;
3. Assess the feasibility of policymakers applying a modified risk management framework to specific sectors, identifying the assumptions, data, and remaining parameters required to do so – with an initial application focused on cybersecurity policymaking options in a specified sector; and
4. Outline the benefits and limitations associated with using the framework to assess a broader range of policy tools, sectors, and risk mitigation or reduction measures.

## 5. Technical Approach / Analytic Methodology

In support of ONCD's efforts to enhance the security and resilience of our digital ecosystem, this study should:

TASK 5.1 – **Identify and assess risk management frameworks used by federal agencies and critical infrastructure owners and operators as well as related cybersecurity practices used to mitigate risks, including:**

- a literature review of existing risk management frameworks to measure the consequences to businesses and national security from cyber incidents as well as identification of cybersecurity practices and other measures used by entitles to reduce risk;
    - an evaluation of any gaps in current literature to measure business or social and national security risk;
    - an assessment of these frameworks to consider variations in methods and data used, risk factors, their components and associated metrics;
- an analysis of the types of factors critical infrastructure owners and operators consider when evaluating and responding to risk, including whether those factors differ across sectors or across organizations within a sector;
- a description of metrics, both quantitative and qualitative, CI owners and operators use to evaluate risk to their organization, including heterogeneity across sectors;
- analysis of cybersecurity practices used to mitigate risks and approaches that federal agencies can incentivize to reduce risk to society or national security; and
- an analysis of organizations' prioritization of funding to address identified risks.

TASK 5.2 – **Update an existing framework and/or develop a new framework to inform how policy incentives can impact decision-making among CI owners and operators with respect to business, social, and national security risks.**

This work will consider findings from Task 1, including observed variations among CI sectors and firms related to risk management methods and data used, risk factors, their components and associated metrics. This framework will consider:

- how dependencies between organizations and/or sectors factor into risk evaluations, particularly when evaluating consequences to the business;
- gaps between business risk mitigation measures and social/national security risk mitigation measures;
- ways in which business and social/national security risk mitigation efforts may or may not overlap;
- conditions under which federal policy may incentivize behavioral change to achieve desired risk mitigation or reduction strategies; and
- factors that may influence heterogeneity across organizations or sectors in levels of compliance, investment in risk mitigation measures, and economic benefit or loss realized by organizations.

TASK 5.3 – **Assess the feasibility of applying the framework developed in Task 5.2. Conduct a case study to apply the framework to a cybersecurity specific application for a critical infrastructure sector or subsector, including:**

- identification of necessary assumptions as well as remaining data and knowledge gaps;
- an analysis of any sector-specific considerations;
- an assessment of whether the framework developed under Task 2 must be refined to better accommodate practical decision-making within the identified sector; and,
- specific recommendations for additional incentives to close identified gaps.

TASK 5.4 – **Outline the benefits, limitations, and potential hurdles associated with using the framework to assess a broader range of policy tools, sectors, and risk mitigation or reduction measures, by:**

- discussing the generalizability of the framework applied in Task 5.3;
- identifying known strengths and weaknesses of the framework; and
- where possible, assessing the plausibility of assumptions and quality/availability of data requirements for framework application.

## 6. Key Words

Risk management framework; economic risk; national security risk; critical infrastructure case study

Type of Work

Risk Management Framework Development

Benefit of Work

Improve risk management; understand risk management frameworks for economic and societal risks

Subject of Interest

Cybersecurity; critical infrastructure resilience; national security risk management

## 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: 1.41

DHS Management Directive 143-04, "Establishing or Contracting with FFRDCs and National Laboratories" defines an 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: Counter Terrorism and Prevent Threats | Mission 2: Secure and Manage Our Borders | Mission 3: Administer the Nation's Immigration System | Mission 4: Secure Cyberspace and Critical Infrastructure | Mission 5: Build a Resilient Nation and Respond to Incidents | Mission 6: Combat Crimes of Exploitation and Protect Victims |
|---|---|---|---|---|---|---|
| 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 | 0% | 0% | 0% | 50% | 0% | 0% |
| 4: Homeland Security Threat and Opportunity Studies | 0% | 0% | 0% | 50% | 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 | Planned Dissemination (See Section 15 for more details) | Delivery Date |
|---|---|---|---|
| All | Project Management Plan (PMP) (Draft) | Internal Use | 15 days after award |
| All | Project Management Plan (PMP) (Final) | Internal Use | 25 days after award |
| All | Task Order Project Kickoff Briefing | Internal Use | Within 30 days of project award date |
| **5.1** | Interim Progress Briefing #1 – HSOAC will deliver a briefing with an update on progress and initial | Internal Use | 3 months after award |

| Scope Ref. | Deliverable Name | Planned Dissemination (See Section 15 for more details) | Delivery Date |
|---|---|---|---|
| | observations from Tasks 5.1 including literature review on risk management frameworks. | | |
| **5.2** | Interim Progress Briefing #2 – HSOAC will deliver a briefing with an update on progress and initial observations from Tasks 5.2, including a draft risk framework | Internal Use | 6 months after award |
| **5.3** | Interim Progress Briefing #3 – HSOAC will deliver a briefing with an update on progress and initial observations from Tasks 5.3, including a case study to apply the framework to a cybersecurity specific application. | Internal Use | 9 months after award |
| **5.4** | Interim Progress Briefing #4 – HSOAC will deliver a briefing with an update on progress and initial observations from Tasks 5.4, including benefits, limitations, and potential hurdles associated with using the framework. | Internal Use | 12 months after award |
| **All** | Draft assessment report inclusive of all tasks. | DHS-wide | 12 months after award |
| **All** | Peer-reviewed, revised Assessment Report documenting results of all tasks. | DHS-wide | 14 months after award |

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: Deliverables. 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

### 9.1 Acceptance Criteria:

RAND shall deliver all products concurrently to the Agency/Organization COR/GTM, A/COR, SSPM Acquisition Inbox and CO. Hardcopy (in quantities specified by the ONCD) shall be provided upon request. All products will be scanned for viruses prior to submission. Generally, all work performed under this Task Order shall comply with ONCD Directives, Instructions and Standards. Exceptions may be made on a case-by-case basis.

Completeness – Initial requirements (as identified) are satisfied in all sections.

Accuracy – Documents shall be accurate in presentation, technical content, and adherence to accepted elements of style.

Clarity—Documents shall be clear and concise; project management and terms shall be used, as appropriate. All diagrams shall be easy to understand and be relevant to the supporting narrative.

Specification Validity—all deliverables must satisfy the requirements of the U.S. Government as specified herein.

File Editing—All text and diagrammatic files shall be provided in Microsoft Office Version 2010 or higher (Word, Excel, PowerPoint, Visio, etc.) so that they can be edited by the U.S. Government.

Format—Documents shall be submitted electronically whenever possible. Hardcopies shall be provided upon request. The document's format may change from Subtask to Subtask.

Timeliness—Deliverables shall be submitted on or before the due date specified in the Schedule of Deliverables Section of this SOO or submitted in accordance with a later scheduled date determined solely by the Government.

The COR will notify RAND of deliverable acceptance or provide comments in writing within ten (10) Government workdays of receipt of a deliverable. Within ten (10) Government workdays of receipt of the written comments, RAND shall resubmit the final deliverable to the GTM, COR, and Contracting Officer, if necessary.

### 9.2 Performance Monitoring / Acceptance Criteria:

A. Services

The GTM will review the monthly progress report and consider the following performance metrics in addition to applicable metrics. The results will be inclusion in the overall review of the progress report.

1. Quality of Services
   - Was the work performed and reflected in the report consistent with observations and expectations?
   - Were the deliverables listed in the report for your task order received and accepted (see Deliverable Review criteria)?

2. Timeliness of Delivery
   - Were the deliverables of task orders delivered on time?
   - Were the informal deliverables delivered on time?
   - Was the Task Order performance in accordance with the proposed schedule?

3. Cost Control
   - Task Order hours only: Were the hours incurred commensurate with the work performed? (e.g., projects/task orders reports based on their respective projects).
   - At the end of the fiscal year, the Program Office will compute the variance between dollars awarded and cost incurred. If the overall requirements are reduced or the level of contractor support without formally changing the task order value, the variance will not be considered in the analysis.

     Satisfactory: 70% of the variances will be less than 10% (plus or minus)
     Very Good: 80% of the variances will be less than 10% (plus or minus)
     Excellent: 90% of the variances will be less than 10% (plus or minus)

### 10. Travel

Travel may be necessary to meet and coordinate interagency exchanges of information and to collect data for this task. Travel includes specific trips for the RAND staff to the DC region to facilitate in-person engagements as specified by the Engagement Plan. 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 |
|---|---|---|---|
| Los Angeles, CA | Washington DC | 2 | 4 |
| Pittsburgh, PA | Washington DC | 2 | 4 |

- Total Number of Trips (All Travelers): 4
- Total Number of Travel Days (All Travelers): 16

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 fourteen (14) months from date of task order award.

### 12. Security Requirements.

This Task Order will require access to the following information:

☒ 1. Unclassified, no markings
☒ 2. Sensitive but Unclassified (SBU), For Official Use Only (FOUO)
☒ 4. Personally Identifiable Information (PII)
☒ 5. Protected Critical Infrastructure Information (PCII)

**12.1** 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.

**12.2** 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 a 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

The FFRDC team will use its 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, 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

N/A

### 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.

**Data Management:**

The FFRDC will require access to the types of CUI listed at the beginning of the Security Requirements section for the purpose of completing the tasks listed above. CUI will be stored and remain in the FFRDC IT Enclave.

The FFRDC will require recurring access to government facilities. The FFRDC will retain CUI in accordance with the applicable records schedule. To support the long-term needs of the Department as its FFRDC for studies and analysis, HSOAC will retain the data over the period of performance of the FFRDC IDIQ 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.

## 13. Safeguarding/Storage:

a. CONFIDENTIAL level safeguarding/storage is 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 of approval(s) to the FFRDC.

The FFRDC may interview and conduct workshops of recognized subject-matter experts, including non-federal experts, to gather the experts' 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 any way. 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.

- If you don't want to release the results, is the FFRDC able to release info about the methodology to the other DHS components or the public?
  *No.*
- Do you want an outreach event as part of the release?
  *No.*
- Would you be interested in having the S&T FFRDC PMO assist with the release of favorable results?
  *No.*

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

If work at Office of the National Cyber Director 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 FFRDC personnel.

DHS Furnished Property – a quarterly report of all S&T property should be submitted to the COR | FFRDC of all 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. EOP / ONCD Furnished Facilities, Supplies and Services

Government furnished property (materials, equipment, and/or information) will be provided in conjunction with required performance under this task order as determined by mutual agreement between the Government and RAND. RAND purchase of hardware or software tools, unless approved as part of the task order for this Proposal, must be preapproved by the GTM.

At the written request of the Government, RAND will immediately return any property provided by the Government for RAND's use and completion of assigned tasks. If not requested, RAND will continue to abide by FAR Part 45 until completion of the Task Order or contract.

The Government will arrange for RAND access to ONCD data, previous studies or information that was used as a basis for development of the IRS business systems, works in progress, deliverables, and other materials essential to perform independent assessments or other activities in support of this Proposal. This information will include, but not be limited to, requirements and architecture documentation, budget and expenditures information, and various planning and CONOPS documentation for the projects under study.

Contractor workspace will be provided to RAND personnel under this task order if available. Individual RAND personnel will be provided access to ONCD data and network capabilities as determined by the ONCD after the appropriate HSPD-12 requirements have been satisfied.

### 18. Invoices

HSOAC: Invoices are due on the 20th of each month.

### 19. Points of Contact

| Government POCs | Corresponding FFRDC POCs |
|---|---|
| **Program Manager**<br>[redacted]<br>Business Operations Manager<br>FFRDC PMO<br>[redacted] | **FFRDC Task Lead**<br>[redacted]<br>Policy Researcher, Sr<br>RAND Corporation<br>[redacted] |
| **Contracting Officer's Representative**<br>[redacted]<br>Business Operations Manager<br>FFRDC PMO<br>[redacted] | **FFRDC Program Director/Portfolio Manager**<br>[redacted]<br>Acting Director, Infrastructure, Immigration, and Security Operations Program, HSOAC<br>Senior Policy Researcher, RAND Corporation<br>[redacted] |
| **Contract Officer**<br>[redacted]<br>Contracting Officer<br>DHS/MGMT/OPO<br>[redacted] | **FFRDC Contracts Lead/Manager**<br>[redacted]<br>HSOAC Contract Administrator<br>RAND<br>[redacted] |
| **Suitability/Fitness Point of Contact**<br>[redacted]<br>Security Specialist<br>DHS S&T\OES\ASD\SPCO<br>[redacted] | **FFRDC Security Staff**<br>Terri Ventrone & Nate Shoemaker<br>[redacted] |
| **Additional Points of Contact (Optional)** | **Notes:** |
| **Program Manager**<br>**Name:** [redacted]<br>**Title:** Director, National Cyber Policy & Programs<br>**Organization:** EOP / ONCD<br>**Phone Number:** [redacted]<br>**Email Address:** [redacted] | |
| **Contracting Officer's Representative**<br>**Name:** [redacted]<br>**Title:** Budget Analyst<br>**Organization:** EOP / ONCD<br>**Phone Number:** [redacted]<br>**Email Address:** [redacted] | |
| **Contract Officer**<br>**Name:** [redacted]<br>**Title:** Team Lead / Contracting Officer<br>**Organization:** EOP / Office of Administration (OA)<br>**Phone Number:** [redacted]<br>**Email Address:** [redacted] | |
| **Alternate (PM, COR, etc.)**<br>Name: [redacted]<br>Title: Contract Specialist<br>Organization: EOP / Office of Administration (OA)<br>Phone Number [redacted]<br>Email Address [redacted] | |