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

U.S. Department of Homeland Security

Online Facilitated Identity Theft and Fraud Victimization

Component/Office: OSE/TCD
Directorate/Division: Science & Technology (S&T)
FFRDC: Homeland Security Operational Analysis Center (HSOAC)

Version: 1.1

Date: October 7, 2024

1. Challenge

In 2021, about 23.9 million U.S. adults had experienced identity theft in the past 12 months, and in situations where the victim knew the cause, 38% claimed the fraud was committed online.[1] Furthermore, internet crimes reported to the FBI show more than $10 billion dollars in loss in 2021, from over 800,000 separate reports.[2] Similarly, the FTC reported $8.8 billion in financial losses in 2021, based on over 2.4 million consumer reports related to many forms of identity theft, government and benefits fraud, and other online scams.[3]

These forms of online identity theft and fraud are activities that take place wholly or partially online, and can damage an individual's social, emotional, psychological, financial, or even physical safety. Victims of online fraud can incur difficulty when applying for loans, other governmental benefits, filing income tax returns, suffer evictions or difficulty securing housing.

In some cases, perpetrators trick victims into sending money or giving out personal information to perpetuate the fraud. For example, fraudsters have targeted disaster survivors by masquerading as FEMA agents in order to collect personal information from the victim. Beyond denying the victim critical recovery funds for an immediate need, little else is known about what becomes of these victims when they need to apply for, or access, government benefits.

And with more of our lives taking place online, the opportunities for identity theft and fraud are increasing.

---

[1] See 2021 BJS Identity theft report, https://bjs.ojp.gov/document/vit21_sum.pdf, last accessed December 11, 2023.

[2] See https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf, last accessed December 11, 2023. Note that these crimes include phishing, business email compromise, and breaches of personal information.

[3] See https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf, last accessed December 11, 2023.

2. Outcome(s)

At the conclusion of this project, DHS S&T will have a better understanding of the rates and forms of online identity theft, types of victims, and variations and magnitudes of harms they suffer, such as emotional distress, loss of money, hopelessness, and loss of trust. S&T will also better understand the forms of redress available to victims and how the harms impact DHS equities and components.

Previous studies on this topic have been domain specific such as the NCVS study on victim of identity theft, and conducted mostly to understand the incidence, prevalence and estimate the financial losses due to identity theft. The proposed research will take an interdisciplinary approach drawing from social science, computer science, cybersecurity, criminology, and economics.

3. Background

In recent years, the White House has taken a number of important steps to investigate, understand, and mitigate individual harms resulting from online fraud and abuse. For example, in June 2022, the White House established a task force to prevent and mitigate harms from online harassment and abuse.[4] In March 2023, it issued its blueprint to address online harassment and abuse,[5] which included efforts to improve digital equity across the country, provide additional training for law enforcement, prosecutors, and victim services. The blueprint also called on the National Institutes of Health and Federal Communications Commission to also investigate and address these harms.

While past research described risk factors and prevalence for online identity theft and fraud victimization generally, there is a dearth of information regarding non-financial harms. For instance, a small body of research shows that online romance and trust fraud can impart lasting damage to victims' physical health, mental health, and overall well-being, with some victims experiencing ongoing depression and anger (Cross et al., 2016; Cross, 2018).[6] Despite the online nature of the relationship, victims of relationship fraud often fear further victimization, even fearing for their physical safety (Cross & Lee, 2022; Cross et al., 2016).[7] Victims have been characterized as experiencing a "double hit," being faced with both financial loss and the loss of a perceived relationship, and even blaming themselves, further exacerbating the negative impacts (Cross et al., 2016; Luekfeldt, Notté & Malsch, 2020; Whitty & Buchanan, 2016).[8]

---

[4] See https://www.whitehouse.gov/briefing-room/presidential-actions/2022/06/16/memorandum-on-the-establishment-of-the-white-house-task-force-to-address-online-harassment-and-abuse/, last accessed December 11, 2023.

[5] See https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/03/executive-summary-initial-blueprint-for-the-white-house-task-force-to-address-online-harassment-and-abuse/, last accessed December 11, 2023.

[6] See Cross, Cassandra, Richards, Kelly, and Smith, Russell (2016), Improving Responses to Online Fraud Victims: An Examination of Reporting and Support, Report to the Criminology Research Advisory Council and Cross, Cassandra (2018), (Mis)Understanding the Impact of Online Fraud: Implications for Victim Assistance Schemes, Victims & Offenders, 13(6), 757-776.

[7] See ibid and Cross, Cassandra, and Lee, Murray (2022), Exploring Fear of Crime for Those Targeted by Romance Fraud, Victims & Offenders, 17(5), 735-755.

[8] See ibid, and See Cross, Cassandra, Richards, Kelly, and Smith, Russell (2016), Improving Responses to Online Fraud Victims: An Examination of Reporting and Support, Report to the Criminology Research Advisory Council, Leukfeldt, Eric Rutger, Notté, R. J. and Malsh, M. (2019). Exploring the Needs of Victims of Cyber-dependent and

4. Task Objective(s)

The U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T) seeks research to help inform efforts to detect, understand, characterize, and differentiate the impacts of online facilitated identity theft/fraud on victims in the U.S. In particular, it seeks to understand the state of current literature and knowledge regarding prevalence, forms, as well as the direct (often financial) and indirect (e.g., emotional, life opportunities and happiness, etc.) harms resulted from these crimes.

S&T is also interested in understanding how online identity theft and fraud affects DHS missions and operations, such as to FEMA when providing benefits to help the families and survivors affected by disasters, or other DHS missions such as immigration or border protection.

To support DHS in meeting this challenge, HSOAC will provide technical expertise and assessment regarding understanding:

- What are the financial and *non-financial* harms of identity fraud such as irreparable credit scores, eviction, inability to access government services, physical health problems, emotional problems like fraud trauma syndrome, and psychological distress?
- What are current remedies for online facilitated identity theft/fraud and what are gaps in remedies (e.g., credit monitoring, education services, victim services, civil remedies) for victims?
- We will also examine, to the extent possible, following two issues:
    - The degree to which online facilitated identify theft and fraud impacts DHS operations, such as:
        - FEMA benefits issuance programs and emergency assistance programs
        - Investigations by USSS and ICE/HSI
        - TSA operations trusted traveler programs
        - Immigration applications
        - Visa Programs
        - CBP and border processes
    - Emerging types of online facilitated identity thefts/frauds (such as synthetic identity theft in which multiple people's personally identifying information is used to create new, synthetic identities; online auction frauds, and frauds in disaster regions).

5. Technical Approach / Analytic Methodology

To meet the objectives of this effort, the work will be organized into the following subtasks:

5.1 Literature Review

HSOAC will conduct a literature review of the existing body of research across multiple domains to address the above research questions. The literature review will focus on the types of online facilitated thefts/frauds; the financial and non-financial harms suffered by victims; victim awareness of victimization and victim reporting; remedies for victims for identify fraud; and potential impacts on DHS operations. The literature review strategy will be developed in consultation with a RAND research librarian and will include academic, gray-literature, and policy documents.

Cyber-enabled Crimes, Victims & Offenders, 15(1), 60-77, and Whitty, Monica T., and Buchanan, Tom (2015), The Online Dating Romance Scam: The Psychological Impact on Victims – Both Financial and Non-Financial, Criminology & Criminal Justice, 16(2), 176-194.

5.2 Landscape Analysis

HSOAC will conduct a landscape analysis of online facilitated identity theft/fraud using publicly available data. Our analysis will identify the forms of online facilitated identity theft/fraud; prevalence of these frauds; and the types and magnitude of harms experienced by victims (to include both monetary and non-monetary harms. Our analysis will rely on the following data sources:

- Federal dockets of online facilitated identity theft/fraud cases
- Victim reports from the Federal Trade Commission (FTC), the FBI's Internet Crime Complaint Center (IC3), and https://gaoinnovations.gov/
- Data breach incidents from the Identity Theft Resource Center and/or the Privacy Rights Clearinghouse
- Pandemic Benefits fraud, https://www.pandemicoversight.gov/.

Where possible, HSOAC will include other data sources identified through the literature review or in consultation with the sponsor.

The analysis of court dockets will combine human coding and Natural Language Processing (NLP) approaches to negotiate tradeoffs between detailed analysis and the number of cases considered. The authoritative source used to identify federally prosecuted cases will be the Federal Judicial Center's Integrated Database (IDB). The Federal Judicial Center was established by Congress in 1967 (28 U.S.C. §§ 620–629) and is the "research and education agency of the judicial branch of the U.S. government." The IDB contains data on all "civil case and criminal defendant filings and terminations in the district courts, along with bankruptcy court and appellate court case information" and represents an exhaustive set of all criminal cases prosecuted in U.S. federal courts.

HSOAC will develop criteria for selecting cases and develop a sampling strategy (stratified by year and circuit) to collect an appropriate number of online facilitated theft/fraud cases. Once the set of cases is identified, we will locate each case in the federal criminal document management system, PACER (Public Access to Court Electronic Records), and will download relevant pleadings and judicial filings using automated techniques. In order to support the analysis in subsequent steps, we will clean the data, and code properties related to the victim, harms to the victim, the offender, type and manner of alleged offenses, metadata related to the court/jurisdiction, and other case properties.

This approach of coding properties of a lawsuit for empirical analysis (sometimes referred to "docketology") builds on HSOAC's past capabilities, and will involve both manual and automated (i.e., NLP) techniques. After we have generated a dataset, we will quantitatively analyze it in order to identify the financial and non-financial impacts of online facilitated fraud/theft, as well as other case characteristics, such as victim remedies.

5.3. Case Study

As applicable, based on findings from tasks 5.1 and 5.2, HSOAC will develop a detailed case study articulating how online facilitated identity theft/fraud has impacted victim access to/use of DHS services.

5.4 Interviews

HSOAC will also conduct semi-structured interviews with DHS staff and other subject matter experts (such as other federal agencies) in order to identify how the harms and abuses from online identity theft may affect DHS equities and components. HSOAC will work with the sponsor in order to identify the appropriate sample of DHS employees to interview.

5.5. Document Results

HSOAC will produce a public report describing the findings from tasks 5.1-5.4. The report will describe the existing research on online facilitated identity theft/fraud, findings from the landscape analysis, and recommendations for mitigating these impacts and/or for future research needs.

HSOAC will also consider producing derivative information products and graphics that include summaries of the findings and insights.

HSOAC will contribute victimology, harms and other concepts to enrich an existing DHS S&T anti-fraud ontology. The ontology contribution will bolster the ontology with new concepts, relationship types, from a victim focused perspective.

Pursuant to sections D.3 and D.6 of the FFRDC contract, HSOAC will publish and publicly release the final report so long as it does not contain "sensitive information" as that term is defined in the contract. In the event the final report must contain sensitive information, HSOAC will produce a short, non-sensitive, publicly releasable report or white paper (i.e., RAND Perspective) as a derivative companion product.

6. Key Words

Type of Work

Landscape analysis, literature review, case study

Benefit of Work

Address knowledge gap in harms of online identity theft, identify impact of online identify theft/fraud on DHS operations, improve victim access to DHS services

Subject of Interest

Identity theft/fraud, online facilitated crime, victimology.

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: 0.85

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%	0%	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%	100%	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[9]

Scope Ref.	Deliverable Name	Delivery Date
All	Project Management Plan (PMP) (Draft) <<Note IDIQ Requirement>>	15 days after award
All	Project Management Plan (PMP) (Final) <<Note IDIQ Requirement>>	30 days after award

[9] The deliverable schedule presented assumes that the sponsor will recognize the current DHS fitness status of RAND team members in accordance DHS Instruction 121-01-007-01. Should the sponsor require additional fitness procedures that take longer than 5 working days, the deliverable schedule shall be revised such that the due dates are extended to include the time for fitness determinations by the sponsor.

All	Task Order Project Kickoff Briefing <<Note IDIQ Requirement>>	Within 30 days of project award date
5.1	Deliverable: Draft Literature Review	5 months after award
5.2	Interim Project Review	7 months after award
5.3	Deliverable: Landscape Analysis Results Briefing	9 months after award
5.4	Deliverable: Draft Case Study, and Interim Project Review	11 months after award
5.5	Deliverable: Draft Report	12 months after award
5.6	Deliverable: Final Report	18 months after award (end of 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

None

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, DC	San Francisco	2	4

These 2 trips are allocated for the PIs to attend and optionally present this research at the Annual Association of Criminology Society conference to be hosted in San Francisco in November (https://asc41.org/events/asc-annual-meeting/).

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 << DELETE NON-APPLICABLE BOXES – doing this streamlines Appendix G submissions >>:

☒ 1. Unclassified, no markings
☒ 4. 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 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.

12.3 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

N/A

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.

Data Management

HSOAC will require access to personally identifiable information (PII) for the purpose of conducting interviews and a landscape analysis of online facilitated identity theft/fraud using publicly available data. CUI will be stored and remain in the HSOAC IT Enclave.

HSOAC will not require recurring access to government facilities. HSOAC will retain CUI in accordance with the applicable Federal 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.

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.

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

  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.

- 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?

  To increase the value of this analysis to the sponsor and DHS, the sponsor is interested in broad sharing of methodologies developed in this task to DHS components and the public. Sharing descriptions of methodologies will allow DHS and its research and analysis partners to extend and further utilize the methods developed in this task in the future. Such descriptions should not reveal DHS Sensitive Data, should not describe the results of DHS or FFRDC assessments of DHS programs or operations, and should not state DHS policy positions. Examples of mechanisms for sharing descriptions of methodologies include but are not limited to HSOAC publications, peer-reviewed journal articles, academic conference presentations, and industry events.

- 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, DHS oversight organizations, 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.

- Do you want an outreach event as part of the release?

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

- Would you be interested in having the PMO assist with the release of favorable results?

  To increase the benefit of this work, the sponsor welcomes assistance from the PMO to complement HSOAC and sponsor dissemination of results. As dissemination

planning proceeds throughout the study, the sponsor will work with HSOAC to identify opportunities to leverage the PMO to enhance the dissemination strategy and include the PMO into the planning process appropriately.

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

If work at *<< insert DHS component name >>* 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] Lead Social Scientist DHS Social Science Technology Center [redacted]	**FFRDC Task Lead** [redacted] Senior Policy Researcher The RAND Corporation [redacted]
Contracting Officer's Representative [redacted] FFRDC PMO COR DHS S&T/OIC/FFRDC [redacted]	**FFRDC Program Director/Portfolio Manager** [redacted] Acting Director, Management, Technology & Capabilities Program 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]

<< 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	