Privacy Impact Assessment

for the

DHS Federally Funded Research and Development Centers

DHS Reference No. DHS/S&T/PIA-042

September 7, 2021

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) sponsors federally funded research and development centers (FFRDC). The DHS Science and Technology Directorate (S&T) FFRDC Program Management Office (PMO) oversees and manages access to these specialized services in systems engineering, integration, studies, and analysis. The FFRDC services can be accessed by DHS components; external federal, state, and local government; non-governmental organizations and institutions; universities and affiliated research centers; and other public sector and private sector groups, through the PMO. S&T conducted this Privacy Impact Assessment (PIA) to address the Department's FFRDC program as well as two specific FFRDCs (i.e., Homeland Security Operational Analysis Center [HSOAC] and Homeland Security Systems Engineering and Development Institute [HSSEDI]) and the privacy risks associated with the collection, use, maintenance, and dissemination of personally identifiable information (PII), privacy sensitive projects and activities, and use of DHS-accredited information systems.

Introduction

Federally Funded Research Development Centers (FFRDC)

Federally funded research development centers are staffed with leading experts and researchers that cover policy, strategy, analytics, systems engineering, technology, and other disciplines to further the government's mission. FFRDCs are sponsored by the U.S. Government and operated by contractors to meet a specific long-term research or development need that cannot be met as effectively by existing in-house or contractor resources. FFRDCs are not-for-profit, private entities that work as trusted advisors in the government's interest and are not permitted to engage in competition for federal procurement contracting.

This PIA focuses on two DHS-sponsored FFRDCs[1] that are categorized into one of two functional purposes: (1) systems engineering and integration (Homeland Security Systems Engineering and Development Institute operated by the MITRE Corporation); and (2) studies and analysis (Homeland Security Operational Analysis Center operated by the RAND Corporation). A third DHS-sponsored FFRDC is a research and development laboratory, the National Biodefense Analysis and Countermeasures Center. The National Biodefense Analysis and Countermeasures Center FFRDC is addressed in a separate PIA.[2] Each FFRDC has a sponsoring agreement defining the FFRDC's focus areas, or core competencies, which reflects their comprehensive knowledge of the sponsor's needs. The FFRDC sponsoring agreements define the methods of how the

[1] *See* https://www.dhs.gov/science-and-technology/ffrdcs.
[2] NBACC is discussed in separate privacy compliance documentation. For more information on NBACC and NBACC systems, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, SCIENCE AND TECHNOLOGY DIRECTORATE, PRIVACY IMPACT ASSESSMENT FOR THE GENOMIC DATA NETWORK AND ANALYSIS (GDNA), DHS/S&T/PIA-039, *available at* https://www.dhs.gov/privacy-documents-st.

government will obtain services from the FFRDC and who can use its services. To that end, DHS-sponsored FFRDC services can also be accessed by other federal, state, local, and tribal government entities, through engagement with the FFRDC-Program Management Office. As documented in the FFRDC ordering guide procedures (further discussed below), program managers for DHS components accessing services of the FFRDCs are required to coordinate with the appropriate DHS component privacy office to determine if a Privacy Threshold Analysis (PTA) is required prior to the start of performance. When a PTA is required, the FFRDC supports the development of compliance related documentation and meets privacy requirements. The DHS sponsoring component will conduct any other privacy compliance review if the work impacts that component's operational decisions or services. This PIA does not cover operational activities; therefore, the DHS component privacy office must determine if the FFRDC is performing operational activities that require separate PIA coverage.

Pursuant to the Homeland Security Act[3] and DHS guidance,[4] the FFRDC work is closely associated with inherently governmental functions by providing analysis and recommending solutions, which are critical to the DHS mission and operations. The primary objective of these DHS-sponsored FFRDCs is to provide the Department with independent and objective advice on critical issues throughout the homeland security enterprise. The FFRDCs ensure the projects and systems managed and operated, on DHS's behalf, adhere to privacy requirements set forth by overarching policies, procedures, and standards. Privacy requirements include adherence to DHS guidelines and specific statutory requirements under the Privacy Act and applicable U.S. Office of Management and Budget (OMB) guidance on managing information as a strategic resource. For example, a DHS component privacy office may determine that a data set used in FFRDC research is subject to the Privacy Act and requires an applicable System of Records Notice (SORN). The privacy analysis will ensure that the FFRDC's use of the record is compatible with the purpose for which the record was collected.

Each FFRDC's architecture is designed so missions can be complementary and provide balanced support across the Department. The FFRDCs are required to leverage DHS-accredited IT Enclaves (e.g., Homeland Security Systems Engineering and Development Institute or Homeland Security Operational Analysis Center IT Enclaves) and/or an approved DHS environment for performing projects on behalf of DHS. The FFRDCs propose IT environments where the work will be performed in the Technical Execution Plans (TEP). As appropriate, a DHS component privacy office reviews the TEP during the procurement review process, may require the completion of a PTA at that time, and will assist in determining if an alternate IT environment is appropriate for use other than an authorized DHS environment (e.g., HSSEDI/HSOAC IT

[3] 6 U.S.C. § 185.
[4] *See* U.S. Department of Homeland Security, Management Directive 10100.1, Organization of The Office of The Under Secretary for Science and Technology (2007), *available at* https://www.dhs.gov/publication/general-science-and-innovation.

Enclave, other DHS component system). The DHS component privacy office will coordinate with the corresponding Chief Information Security Officer and other appropriate offices during this process. The types of Homeland Security Systems Engineering and Development Institute and Homeland Security Operational Analysis Center IT Enclaves, as well as their respective projects will be discussed in the Addenda to this PIA.

The Homeland Security Systems Engineering and Development Institute and the Homeland Security Operational Analysis Center will use their respective MITRE and RAND IT Enclaves for project information (e.g., financial information related to contract management) and other select project information (e.g., access control requirements), including information owned by DHS components. The Homeland Security Systems Engineering and Development Institute and the Homeland Security Operational Analysis Center will handle data in accordance with the specific guidance from data owners and their appropriate DHS component privacy office. The FFRDC-PMO coordinates all FFRDC activities, which includes ensuring that the appropriate DHS component privacy offices are included in the project review process. This direction begins early in the process of placing a request for the services of the FFRDCs. In addition, the FFRDCs will treat any applicable data collection that pertains to individuals in accordance with the Privacy Act and as required under the contract.

Homeland Security Systems Engineering and Development Institute (HSSEDI)

DHS created HSSEDI to address homeland security system development issues where technical and systems engineering expertise is required. The Homeland Security Systems Engineering and Development Institute FFRDC objectively analyzes homeland security system problems, addresses complex technical questions, and generates creative and cost-effective solutions in strategic areas that impact DHS' missions and priorities such as cybersecurity, border protection, immigration, critical infrastructure protection, and others. With timely, accurate, synthesized data leveraging data analytics, enabling DHS to address today's challenges and set the proper trajectory for future homeland security capabilities is of critical importance. The Homeland Security Systems Engineering and Development Institute FFRDC provides systems engineering and integration expertise to DHS leadership and other homeland security stakeholders as a trusted agent, particularly in the evolution of the most complex and critical homeland security programs. This is accomplished by providing specialized independent and objective technical and systems engineering expertise in the following focus areas and core competencies:

- Acquisition Planning and Development
- Emerging Threats, Concept Exploration, Experimentation and Evaluation
- Information Technology and Communications
- Cyber Solutions / Operations

- Security Systems Engineering, System Architecture and Integration
- Technical Quality and Performance
- Independent Test and Evaluation

The Homeland Security Systems Engineering and Development Institute has developed a DHS-accredited IT Enclave, to include on-premise, cloud services, and other IT related services, to protect DHS information used for its project work in a DHS-accredited environment. The Homeland Security Systems Engineering and Development Institute IT Enclave will have a general support system, Virtual Desktop Infrastructure (VDI) support, and a suite of software applications, such as Microsoft Office products. These systems comprise the Homeland Security Systems Engineering and Development Institute IT Enclave infrastructure that will store basic contact information in support of HSSEDI research and business operations and manage project data.

Homeland Security Operational Analysis Center (HSOAC)

The Homeland Security Operational Analysis Center supports the Department in addressing analytic, operational, and policy challenges in its mission areas and across the homeland security environment. The Homeland Security Operational Analysis Center provides analysis of early-stage activities, portfolio planning and analysis, policy development, acquisition planning, and support for the transition of products into government operations or licensing for use by others. It works across seven focus areas:

- Homeland security threat and opportunity studies that use risk assessment and forecasting to track current threats and identify vulnerabilities and potential future risks;
- Organizational studies that use workforce analysis and performance measurement to help DHS improve unity of effort across management and planning;
- Operational analysis that uses evaluation and simulation methods to help DHS assess mission requirements, improve operational processes and procedures, and understand the impact of operations on a range of outcomes;
- Regulatory, doctrine, and policy studies that use regulatory and policy analysis to offer insight into the potential impact of changes in external regulations, policies, and doctrines on DHS missions and activities;
- Acquisition studies that use planning, program management, and test and evaluation expertise to assess DHS acquisition needs and apply lessons from past experiences;

- Research and development (R&D) studies that use portfolio and foresight analysis to help DHS plan for the mix of projects needed to accomplish its missions and transition R&D results into technology and practice; and
- Innovation and technology acceleration that uses technical analysis to promote integration and adoption of new technologies and identify barriers to adoption.

The Homeland Security Operational Analysis Center has developed a DHS-accredited IT Enclave, to include on-premise, cloud services, and other IT related services, to protect DHS sensitive information used for Homeland Security Operational Analysis Center project work in a DHS-accredited environment. The IT Enclave is currently under development and it is expected to include a general support system, virtual workspaces, and a suite of software applications, such as Microsoft Office products. These systems comprise the Homeland Security Operational Analysis Center IT Enclave infrastructure that will store basic contact information in support of Homeland Security Operational Analysis Center research and business operations and manage project data. The types of Homeland Security Operational Analysis Center IT Enclave project data will be described in further detail in a forthcoming Addendum to this PIA.

HSSEDI and HSOAC Data Collection

For each project, the FFRDCs will collect and access business contact information, to include name, email address, phone number, organization, mailing address, and expertise from stakeholders, such as members of the public, DHS employees and contractors, and individuals from academia, industry, and non-DHS government organizations. The details for each FFRDC engagement and the project data, including PII, will vary. Each project will be documented in a project-specific PTA and will be outlined in the Task Order execution by the Component Program Manager and Contracting Officer Representative. Creating the PTA and other requisite privacy documentation (e.g., PIA, SORN) and obtaining DHS Privacy Office adjudication is the DHS sponsoring organization or component's responsibility.

FFRDCs may collect, maintain, use, store, and share the following types of personal information throughout the various projects from members of the public, DHS employees or contractors, and federal, state, local, and tribal individuals:

- Contact information (e.g., full name, phone number, address, personal email address);
- Personal identifiers (e.g., online identifiers, aliases, usernames);
- Sensitive personal identifiers (e.g., Social Security number, credit card numbers, financial account numbers, passport numbers, A-number);
- Descriptive data (e.g., gender, birthplace, age or date of birth, ethnicity);
- Device information (e.g., IP address, Media Access Control Address, device name);

- Biometric samples (e.g., face images, speech/voice, fingerprints, or other biometric information);
- Biometric data (e.g., Fingerprint Identification Number, biometric templates, typing cadence);
- Medical history and other health-related information;
- Professional information (e.g., education, awards, resumes, occupation); and
- Open-source information (e.g., publicly available information that may be purchased, obtained through a subscription-based service, or is provided free to the public).[5]

Additional PII could be collected as projects are defined for different stakeholders.

Data Sources and Use

FFRDCs are required to leverage the DHS-accredited IT Enclaves and/or an approved DHS environment for performing projects on behalf of DHS. The DHS FFRDC IT Enclaves maintain data from the different sources listed below. The FFRDCs receive, send, and use data only within the scope of established data handling guidance (e.g., Ordering Guide, contracts, TEPs) and in compliance with DHS policies.[6] Appropriate data handling guidance will be developed for each data source via the project-specific PTA outlining the specific project, activities, and related requirements.

- Government Data: In some instances, government data owners associated with different missions and DHS components will make full or limited data sets available for specific research activities. DHS components, other federal agencies, foreign governments, and state, local, or tribal organizations have established authorities to collect and use various data sets related to homeland security missions. For critical DHS missions, and in accordance with DHS authorities, the FFRDCs will receive guidance from government data owners on how specific data should be used, shared, and disposed of accordingly.
- Commercial Data: The FFRDCs may obtain commercial data for specific activities. Projects may examine the use of commercial data, or if there is mutual benefit, may lead to the development of new commercial data services. The FFRDCs also use relevant third-

[5] The FFRDCs are not permitted to use any commercial data for DHS projects or activities without explicit approval from the FFRDC-PMO, Federal Project Leader, and the appropriate DHS component privacy office. Access to social media information and sites requires DHS approval through completion of a PTA. Any activity would be documented in a project-specific PTA and all subsequent privacy requirements would be determined by the DHS component privacy office.

[6] *See* U.S. Department of Homeland Security, DHS 4300A Sensitive Systems Handbook, *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook. DHS 4300A is a series of information security policies, which are the official documents that create and publish Departmental security standards in accordance with DHS Management Directive 140-01, *Information Technology System Security*.

party data collected by non-profit organizations and made available for a fee. The FFRDCs may also use commercial data in its research activities to enrich data it receives from other sources. The FFRDCs are not permitted to use any commercial data for DHS projects or activities without explicit approval from the FFRDC-PMO, Federal Project Leader, and the appropriate DHS component privacy office.

- Research Data: The FFRDCs use research data from government, industry, and academia (e.g., U.S. General Services Administration, Cornell University). The FFRDCs will use appropriate data from these sources, where data has been developed and curated for the furtherance of research and development.
- Open Source Data: The FFRDCs use data sets developed through the collection of open source information. The FFRDCs' activities may evaluate the use of new types of data found in open sources or the use of existing open source data to evaluate new tools. The FFRDCs are not permitted to use any open source data for DHS projects or activities without explicit approval from the FFRDC-PMO, Federal Project Leader, and the appropriate DHS component privacy office.

The use of these data sets is reviewed by the S&T Privacy Office and appropriate DHS component privacy office to ensure data is used in a manner consistent with the data owner's terms of use and DHS guidelines, including specific statutory requirements under the Privacy Act and applicable OMB guidance on managing information as a strategic resource. In addition, the S&T Privacy Office collaborates with the FFRDC-PMO to provide guidance on how the data sources will be used and disclosed to the government. The oversight and guidance mechanisms are the FFRDC Ordering Guide, FFRDC Quarterly Reviews, Independent Government Cost Estimate (IGCE), Indefinite Delivery Indefinite Quantity (IDIQ) contracts, and privacy training.

FFRDC Program Management Office (FFRDC-PMO)

The FFRDC-PMO is a DHS oversight and management program office placed within the S&T Directorate operating on behalf of the Department and works across the DHS Enterprise with all components as a resource to access the services of the Homeland Security Systems Engineering and Development Institute, the Homeland Security Operational Analysis Center, and other federal FFRDCs. The FFRDC-PMO's primary business operations responsibilities are to: (1) execute tactical activities to get task orders awarded; (2) conduct outreach activities to improve awareness; and (3) manage the IDIQ contracts to ensure compliance with policies and procedures.

The FFRDC-PMO condenses required functions throughout the task order lifecycle into one office for greater efficiency and effectiveness. Some of the FFRDC-PMO's key responsibilities include:

- Assisting with requirements documentation;

- Processing financial transactions;
- Identifying and assisting with potential contracting requirements;
- Compiling, submitting, and tracking procurement requisitions;
- Performing Contracting Officer's Representative (COR) duties;
- Providing Appropriateness Reviews;
- Facilitating suitability/fitness submissions, invoice processing, foreign travel approval, and public release;
- Conducting task order and interagency agreement (IAA) close outs;
- Managing deliverables and final reports; and
- Providing department wide training on how to access the FFRDCs resources.

As a tool to help manage the FFRDCs, the FFRDC-PMO maintains a database to store knowledge products and program related information.[7] The FFRDC-PMO database is comprised of lists, libraries, forms, reports, and dashboards, which allows the FFRDC-PMO to enter and track various kinds of FFRDC-PMO related information, including task orders, contract actions, invoices, deliverables, suitability, and taskers. Only S&T staff managing the FFRDC-PMO have access to this database.

FFRDC Ordering Guide

Each FFRDC has an Ordering Guide that is designed to be used by contracting officers, contracting officer representatives, and component program managers for guidance navigating the ordering process for FFRDC task orders. The Ordering Guides contain the information required to use the services of the FFRDCs. The Ordering Guides provide general information, the roles and responsibilities of the major parties involved in the ordering and administration processes, and the procedures for ordering services from each FFRDC. The Ordering Guides list out the appropriate capabilities of each FFRDC as contracting officers, contracting officer representatives, and component program managers explore the potential for leveraging the FFRDCs.

Privacy Coordination

The FFRDC-PMO will inform the Component/Government Program Manager that there is a requirement to coordinate with the appropriate DHS component's privacy office (e.g., CBP, USCIS, S&T) to complete the privacy review and determine if there are additional privacy requirements for the information, technology, projects, or activities. In those instances, the FFRDC

[7] The PII collected in the FFRDC-PMO database for purposes of maintaining a list of all FFRDC staff and a list of individuals who request DHS FFRDC services is covered by DHS/ALL/PIA-006 DHS General Contacts List, *available at* https://www.dhs.gov/publication/general-contact-lists.

shall support the completion of privacy compliance documentation and meet privacy requirements. The privacy review will guide program activities and ensure appropriate privacy coverage in addition to this PIA. S&T Privacy is also briefing the DHS privacy community on their respective responsibilities with regards to FFRDCs. S&T Privacy will update the Addendum to this PIA to account for new types of projects.

Technical Execution Plan (TEP)

The TEP is another tool that the FFRDC-PMO uses to determine whether an FFRDC is appropriate to perform the work. The TEP equates to a statement of work or statement of objectives in contracting but is tailored specifically for the purposes of contracting with the Homeland Security Systems Engineering and Development Institute or Homeland Security Operational Analysis Center. The FFRDC-PMO created a Technical Execution Plan template to ensure consistency (to facilitate Appropriateness Reviews) and conformity (to ensure all necessary information is provided) across all task orders. Key sections of the Plan populated by government users include:

- Challenge – Identify the underlying problem, specific to the task order, that requires an FFRDC's assistance;
- Outcome – Identify what will be possible if success is achieved; and
- Objectives – Identify the accomplishments to be realized by the end of the task order.

The Technical Evaluation Plan helps the FFRDC-PMO to determine whether an FFRDC is appropriate to perform the work. Also, each DHS component privacy office has the opportunity to review each Plan during the procurement request review process, as outlined in the Homeland Security Acquisition Manual (HSAM).[8] During this review, the DHS component privacy office ensures that the collection, use, maintenance, and dissemination of PII is done in accordance with DHS guidelines, including specific statutory requirements under the Privacy Act and applicable OMB guidance on managing information as a strategic resource, or if the project requires additional review as it may be deemed privacy sensitive.

Appropriateness Review Process

All work placed with an FFRDC must be within its established purpose, mission, general scope of effort, or special competency. The FFRDC-PMO provides this Appropriateness Review and certification for all DHS and non-DHS FFRDC use in accordance with DHS Management Directive 143-04.[9] The FFRDC-PMO also provides recommendations on which FFRDC is proper

[8] *See* https://www.dhs.gov/publication/appendices.
[9] *See* U.S. Department of Homeland Security, Management Directive 143-04, Establishing or Contracting with Federally Funded Research and Development Centers (FFRDCs) and National Laboratories, *available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt-directive-143-04-establishing-contracting-federally-funded-r-and-d-centers-national-labs.pdf.

to perform the desired research effort. The steps to the FFRDC-PMO conducting the Appropriateness Review for each project are as follows:

1. The FFRDC-PMO receives a request from a DHS component or external government agency or organization to complete an Appropriateness Review for a:
    a. new task order; or
    b. modification to add additional work to (or increase the scope of) an existing task order if approved by a Contracting Officer.
2. An FFRDC-PMO team member reviews the Technical Evaluation Plan, along with other relevant documentation (such as the IGCE or modifications to task orders) against the following criteria (all of which must be met):
    a. The work is appropriate for an FFRDC;
    b. The work falls within the specified FFRDC's mission, purpose, focus areas, and core competencies;
    c. The work draws on or sustains the strategic special relationship between the FFRDC-PMO and DHS;
    d. The work is free from real or perceived conflicts of interest; and
    e. None of the services to be performed are inherently governmental.
3. An FFRDC-PMO team member provides their recommendation to the FFRDC-PMO Federal Lead for the respective FFRDC along with a written explanation of why the work is appropriate/not appropriate.
4. The FFRDC-PMO Federal Lead conducts secondary review for appropriateness and draws their own conclusion on whether the work is appropriate based on their review of the TEP, IGCE, history of prior work (if applicable), and FFRDC-PMO team member's recommendation.
5. Based on their review, the FFRDC-PMO Federal Lead either:
    a. Signs the Appropriateness Review with written justification; or
    b. If the work is not deemed appropriate, elevates the review to the FFRDC-PMO Director for their consideration along with an explanation of why the work is not considered appropriate.
6. If needed, the FFRDC-PMO Director conducts final review for appropriateness and draws their own conclusion based on their review of the Technical Evaluation Plan, IGCE, and recommendations for why the work was judged not appropriate.

a. The FFRDC-PMO Director makes final determination on whether the work is appropriate or not and provides a written justification.

If the FFRDC-PMO determines that the activity is appropriate for the FFRDCs, the Component/Government Program Manager is advised to engage the appropriate DHS component's privacy office.

FFRDC Quarterly Reviews

The FFRDC-PMO has established a Quarterly Review in which the individual FFRDC briefs FFRDC-PMO staff on the status of projects/programs. In this review, the FFRDC Program Manager provides a detailed overview of project/program progress to date and work that remains to be completed. The Quarterly Review allows for: a) the FFRDC-PMO to ascertain if the projects are within acceptable cost/time/quality limits; b) the FFRDC to share success stories of impactful things learned and produced; and c) the FFRDC-PMO to understand from the FFRDC's perspective what the government needs/wants and how that has evolved from the previous Quarterly Review. An S&T Privacy representative will participate in support of the FFRDC-PMO. During this collaborative review the scope and application of privacy controls are assessed at various points of project execution.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[10] articulates concepts of how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[11]

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[12] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[13] and the Homeland Security

[10] 5 U.S.C. § 552a.
[11] 6 U.S.C. § 142(a)(2).
[12] Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06, "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," *available at* https://www.dhs.gov/privacy-policy-guidance.
[13] 44 U.S.C. § 3501 note.

Act of 2002, Section 222.[14] Given that the FFRDCs are programs rather than a particular information technology system, this PIA is conducted as it relates to the operation of FFRDCs associated with the DHS construct of the FIPPs.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate.

The FFRDCs receive information from external parties, such as government agencies, sponsoring organizations, or publicly available data sources, in order to execute task orders. The FFRDCs may also receive information directly from an individual if the FFRDC is collecting business contact information or conducting a survey. This PIA serves as notice and discusses the overall FFRDC processes, types of information collected, redress procedures, and other privacy risks associated with the FFRDCs. Additionally, DHS S&T has a public-facing website that describes the activities of each FFRDC.[15]

Privacy Risk: There is a risk that the government does not provide transparency to the public that the FFRDCs conduct privacy sensitive research and other activities on behalf of DHS.

Mitigation: This risk is partially mitigated. DHS S&T has a public-facing website that describes the activities of each FFRDC. The public-facing website also includes links to the Homeland Security Systems Engineering and Development Institute[16] and the Homeland Security Operational Analysis Center[17] public-facing websites, which provide further details into their respective activities. MITRE and RAND are identified as the operators of the Homeland Security Systems Engineering and Development Institute and Homeland Security Operational Analysis Center, respectively. Further details about the FFRDCs' activities can be found at the following locations: (1) DHS-Homeland Security Systems Engineering and Development Institute website;[18] (2) DHS-Homeland Security Operational Analysis Center website;[19] (3) MITRE Corporate website;[20] and (4) RAND Corporate website,[21] which are all available to the public. In addition, S&T provides notice through the publication of this PIA, which discusses FFRDC processes, activities, and types of information collected. Lastly, each project-level activity that the FFRDCs

[14] 6 U.S.C. § 142.
[15] *See* https://www.dhs.gov/science-and-technology/ffrdcs.
[16] *See* https://www.mitre.org/centers/homeland-security-systems-engineering-and-development-institute/who-we-are.
[17] *See* https://www.rand.org/hsrd/hsoac.html.
[18] *See* https://www.dhs.gov/science-and-technology/hssedi.
[19] *See* https://www.dhs.gov/science-and-technology/hsoac.
[20] *See* https://www.mitre.org/centers/homeland-security-systems-engineering-and-development-institute/who-we-are/the-hssedi.
[21] *See* https://www.rand.org/hsrd/hsoac.html.

engage in requires a privacy review from the respective DHS component privacy office to develop project-based PTAs, PIAs, and SORNs as appropriate. Those types of engagements are captured in the Addendum to this PIA.

However, because some of the data used by FFRDCs during their research activities is originally collected by other entities or publicly available sources, DHS S&T cannot fully mitigate this risk.

Privacy Risk: There is a risk that individuals are not provided notice that the FFRDCs are using their PII for specific projects.

Mitigation: This risk is mitigated. The publication of this PIA provides notice in part, as it discusses the overall FFRDC processes, types of information collected, and redress procedures associated with this program. However, DHS components, other government agencies, and other organizations provide notice, as applicable for the information they collect and how it will be used/shared. Privacy Act Statements or Privacy Notices are provided during information collections and notices are posted if research is taking place in a public space.

Additionally, the Addendum to this PIA will provide notice of the types of projects and the type of PII used.

2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

FFRDCs receive PII directly from individuals, through surveys or focus groups during research activities; from third parties and external data sources, such as government, commercial, research entities; and open source as described earlier in the PIA. The FFRDCs ensure individual participation by collecting directly from the participant where possible, which allows validation of the content for the voluntary submission. Additionally, the FFRDCs will maintain a record of receipt to document an individual's consent, purchase from a legitimate source, or transfer from an authorized source for a documented use. When appropriate, the FFRDCs adhere to the DHS Human Subjects[22] Review, as administered by the Compliance Assurance Program Office (CAPO), to ensure the protection of human subjects in research conducted or supported by U.S. federal departments and agencies.

For information that the FFRDCs receive from government data owners, access by individuals to their information is governed by the respective data owner's Freedom of Information

[22] *See* U.S. Department of Homeland Security, Management Directive 026-04, Protection of Human Subjects, *available at* https://www.dhs.gov/xlibrary/assets/foia/mgmt-directive-026-04-protection-of-human-subjects.pdf.

Act (FOIA) and/or Privacy Act (PA) request policy, generally outlined in the source agency's PIA or SORN. For information on how the FFRDCs receive or collect data from commercial data providers, research consortia, and open sources, any individual who may desire to access their information may do so by submitting a FOIA or PA request to the DHS FOIA Office:

Privacy Office, Mail Stop 0655
U.S. Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528-065

Further, the DHS/S&T-001 Research, Development, Test, and Evaluation Records SORN contains instructions for accessing information under the "Notification Procedure" section.[23]

Privacy Risk: There is a risk that individuals may not have an opportunity to correct inaccurate data held by an FFRDC.

Mitigation: This risk is partially mitigated. In situations where the FFRDCs are collecting information directly from an individual (e.g., a survey), individuals have the ability to correct their information by contacting the individual FFRDC. However, there are also situations where the FFRDCs are receiving information from a third party. In those situations, the FFRDCs are relying on the accuracy of the information and any redress processes would be undertaken through the source of the information. The use of these data sets is reviewed by the appropriate DHS component privacy office to ensure the data is used in a manner consistent with the data owner's terms of use and DHS guidelines.

3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

FFRDCs are public-private partnerships, which conduct research for the U.S. Government. Federal policy for FFRDCs related to the establishment, use, review, and termination of FFRDCs is set by the Homeland Security Act of 2002, 6 U.S.C. § 185, *Federally Funded Research and Development Centers*, and DHS Management Directive 143-04, *Establishing or Contracting with FFRDCs and National Lab*. Federal policy for FFRDCs is further set by Federal Acquisition Regulations (FAR) part 35.017. Finally, in support of the DHS S&T mission, FFRDCs conduct Research, Development, Test, and Evaluation Records (RDT&E) activities that have potential to benefit critical DHS missions throughout the Components and fulfill its mission responsibilities under 6 U.S.C. § 182, *Responsibilities and Authorities of the Under Secretary for Science and Technology*. Prior to initiating a new project, S&T authorities under 6 U.S.C § 182 are reviewed in conjunction with the requirements set forth in the Privacy Act along with DHS policy to ensure

[23] *See* DHS/S&T-001 Research, Development, Test, and Evaluation Records, 78 Fed. Reg. 3019 (January 15, 2013).

all data sets are properly collected and used.

The FFRDC IT Enclaves, which will process FFRDC project-level information — to include PII — are being accredited under the guidelines of DHS 4300A, *Sensitive Systems Handbook*. The FFRDCs are contractually required to leverage the IT Enclaves and/or an approved DHS environment for performing projects on behalf of DHS. These authorities allow the FFRDCs to collect information for the purpose of providing independent analysis of homeland security issues. Data is collected and used in accordance with authorities that enable research, development, test, and evaluation activities within the FFRDCs or in partnership with the data owner as authorized/approved by the Appropriateness Review.

The FFRDC-PMO also relies on these authorities to collect the necessary information in order to oversee and manage the FFRDCs.

Privacy Risk: There is a risk that the FFRDCs may use information in an activity that was collected or received for a different purpose not compatible with the FFRDC research.

Mitigation: This risk is mitigated. The FFRDC-PMO and DHS component privacy review each project to ensure that the collection and the activity are clearly defined, and that data is not inappropriately repurposed. This privacy review is required before a project may move forward. The FFRDCs have resources across multiple projects in support of DHS components and homeland security stakeholders. This assessment will validate the proper alignment between the FFRDCs' activities and the proposed data sets to support the specific project. In addition, the DHS component privacy office is integrated into the Technical Evaluation Plan process, which reviews every FFRDC project to ensure that the collection, use, maintenance, and dissemination of PII and/or privacy sensitive projects and activities are safeguarded in accordance with DHS guidelines, including specific statutory requirements under the Privacy Act, and applicable OMB guidance on managing information as a strategic resource.

Privacy Risk: There is a risk that the FFRDCs may engage in an activity that goes beyond the scope of DHS authorities.

Mitigation: This risk is mitigated. The following controls are in place to ensure that each FFRDC activity is conducted to align with appropriate DHS legal and policy authorities:

- Each activity that the FFRDC conducts undergoes an Appropriateness Review to ensure that the FFRDC is properly scoped to perform the desired research effort and that the work falls within the specified FFRDC's mission, purpose, focus areas, and core competencies;
- The appropriate DHS component privacy office engages with all stakeholders to determine privacy sensitivities and put project-specific privacy compliance documentation in place. This requirement is also articulated in the FFRDC

Ordering Guide. If an activity extends beyond DHS authorities, the FFRDCs will not be permitted to perform the activity. In addition, the DHS component privacy office is integrated into the TEP process, which reviews every FFRDC project to ensure that the proper protections for PII and/or privacy sensitive projects are applied before the activity commences; and

- When appropriate, a legal review is conducted to ensure that the FFRDC activities align with the authorities that govern collection or execution of work.

4. Principle of Data Minimization

Principle: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

The FFRDCs will retain data in accordance with DHS record schedules. FFRDCs will document data retention requirements in the individual project's Data Catalog. Once the effort has concluded, the FFRDC IT Enclaves must delete or return data sets to the data owner, depending on the data source. Per the DHS/S&T-001 Research, Development, Test and Evaluation Records SORN, PII collected during the project is retained for the duration of the project. At the conclusion of the project, PII is returned to the providing DHS component, through secure methods or destroyed. Some routine, non-sensitive business contact PII (e.g., names, email addresses) of 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. The FFRDC IT Enclaves data holdings will be periodically reviewed to verify that that data requirements are being adhered to appropriately.

Privacy Risk: There is a risk that a sponsoring organization will direct the FFRDCs to collect more information than is necessary to execute task orders.

Mitigation: This risk is mitigated. For the FFRDCs, each project begins with a Technical Evaluation Plan, which outlines the data required for the activity. The activity then undergoes an Appropriateness Review to ensure that the FFRDCs can execute the task order, while aligning with the FFRDC's purpose, focus areas, and core competencies. In addition, the specific types of data being collected will be outlined in project-specific privacy compliance documentation.

The FFRDC-PMO also conducts Quarterly Reviews. In these reviews, the FFRDC Program Manager provides a detailed overview of project/program progress to date and work that remains to be completed. The FFRDC-PMO uses the Quarterly Reviews to ensure that the project is aligned to the Plan. Each Plan is reviewed by the appropriate DHS component privacy office and privacy compliance documentation is completed through project specific PTAs to ensure

adherence to the FIPPs and implementation of proper privacy risk mitigations. The PTA analysis also includes how the data is collected (e.g., surveys, focus groups, external collection), the validity of the research — based on the original purpose — and the overall data handling guidelines to ensure that the collection is properly aligned with project contract requirements and the original purpose.

Privacy Risk: There is a risk that data may reside in government and non-government systems for longer than necessary because the FFRDCs do not have a NARA-approved retention schedule or automated data destruction process.

Mitigation: This risk is mitigated. The Homeland Security Systems Engineering and Development Institute and Homeland Security Operational Analysis Center IT Enclaves will process and maintain the following types of federal records:

- DHS research-generated data, to include information generated by the FFRDCs on behalf of the government, which fall within the following existing systems of records as set out in the following SORNs: (1) DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)[24] — covering information collected in order to provide authorized individuals with access to DHS information technology resources; (2) DHS/ALL-026 Personal Identity Verification Management System[25] — covering the personal security information collected about personnel in the system; (3) DHS/ALL-037 E-Authentication Records System of Records[26] — covering information collected by programs and applications for the functions required to enroll, issue, and maintain a credential on DHS's behalf; (4) DHS/ALL-042 Personnel Networking and Collaboration System of Records[27] — covering records containing biographic information of employees and contractors of DHS for the purpose of professional networking and employee collaboration; or (5) DHS/S&T-001 Research, Development, Test, and Evaluation Records (RDT&E)[28] — covering records collected in support of, or during the conduct of, S&T-funded research, development, test, and evaluation activities, and are subject to the NARA-approved records retention schedules associated with each SORN and the disposition instructions for each schedule; and
- Component-generated data, which will fall within applicable existing Component systems of records and their respective SORNs.

[24] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 Fed. Reg. 70792 (November 27, 2012).
[25] *See* DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 Fed. Reg. 30301 (June 25, 2009).
[26] *See* DHS/ALL-037 E-Authentication Records System of Records, 79 Fed. Reg. 46857 (August 11, 2014).
[27] *See* DHS/ALL-042 Personnel Networking and Collaboration System of Records, 83 Fed. Reg. 8685 (February 28, 2018).
[28] *See* DHS/S&T-001 Research, Development, Test, and Evaluation Records, 78 Fed. Reg. 3019 (January 15, 2013).

If a Privacy Act record does not fall within an existing system of records and a new or modified system of records is created, DHS or the appropriate Component will publish a new or modified SORN identifying the associated NARA-approved records schedule or a pending records schedule request. The FFRDC-PMO requires the FFRDCs to coordinate with the Department to identify the applicable systems of records and records retention schedules to ensure that the data is retained and disposed of properly. As part of this mitigation, the FFRDC-PMO requires the FFRDCs to issue data handling plans identifying the relevant retention and disposition requirements and submit disposal certificates to the FFRDC-PMO that account for the lifecycle of the data. The IT Enclaves have the capability to support secure automated disposal of sensitive information, including privacy-sensitive information, that is no longer needed or has reached the end of its retention period in accordance with NIST standards and NARA-approved disposal instructions.

5. Principle of Use Limitation

Principle: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

The FFRDCs conduct research activities, which can include either privacy sensitive technologies or privacy sensitive data. Each FFRDC project undergoes a privacy review that includes a determination of whether the activity is privacy sensitive. If an activity is deemed privacy sensitive, specific requirements limiting the use of information are imposed.

Privacy Risk: There is a risk that information may be used inconsistently with the original purpose of collection.

Mitigation: This risk is mitigated. There are internal administrative controls (e.g., FFRDC Ordering Guide, TEP, Appropriateness Review, and privacy review) that govern the use of FFRDC services to ensure that information is used in accordance with the original purpose of collection.

First, to support this process, the FFRDC Ordering Guide is used to access the services of the FFRDCs. The primary purposes of the FFRDC Ordering Guide are to: 1) provide information about the capabilities of the FFRDC as they explore the potential for leveraging DHS enterprise resources; 2) provide DHS component program managers, contracting officers, and contract specialists with guidance and policies for placing task orders under the DHS contract with the operators of the Homeland Security Systems Engineering and Development Institute and the Homeland Security Operational Analysis Center; and 3) provide users of FFRDC services with the appropriate privacy guidance specific to the respective DHS component.

In addition, the Plan specifically outlines the purposes of the activity and is reviewed during the Appropriateness Review process to determine whether an FFRDC is appropriate to perform the work. The FFRDCs, with the appropriate component program manager, work with their

respective DHS component privacy officer to conduct privacy compliance reviews. DHS component privacy offices are integrated into the Technical Evaluation Plan process, which allows FFRDC projects to be reviewed and ensures that the proper protections for PII and/or privacy sensitive projects are applied before activity commences.

Privacy Risk: There is a risk that records may be shared inappropriately outside of the Department.

Mitigation: The risk is mitigated. Access to FFRDC information is limited to authorized personnel with a need to know and information is generally not shared outside DHS unless included in a document released through the DHS public release process. Any information shared outside of the Department would be automatically documented using the FFRDC IT Enclaves system logs. In addition, DHS has set policy and requirements for Information Sharing and Safeguarding[29] for internal and external use cases, which minimizes the risk of improper sharing. This Departmental policy and governance framework applies to the Department and external entities. The FFRDC work is closely associated with inherently governmental functions and the FFRDC IT Enclaves will process DHS information, which requires the FFRDCs to comply with DHS policies, processes, standards, and guidelines.

Privacy Risk: There is a risk that DHS and a non-DHS sponsors' information will be comingled in the IT Enclaves.

Mitigation: This risk is mitigated. All projects are segregated in both principle and policy, segmenting storage and access of any given data set. There will be physical and logical boundaries to ensure the data sets are used for the specific purpose of the collection and no data sets will be comingled or used without an authorized purpose in coordination with the FFRDC-PMO and in consultation with the appropriate DHS component privacy office. Only individuals with the proper need to know will have access to information.

Privacy Risk: There is a risk of unauthorized access to or improper use of the FFRDC IT Enclaves and data therein.

Mitigation: This risk is mitigated. The FFRDC IT Enclaves manage user access through technical controls and business processes. For example, to access the on-premise environment, an IT Enclave guest must be escorted at all times. Logs of guests and the purpose of their visit are maintained for accountability. To access an FFRDC IT Enclave cloud-based security boundary, a user must meet DHS suitability requirements, be issued a Personal Identification Verification (PIV) card, and be actively supporting an FFRDC project. Authorized FFRDC IT Enclave users are required to sign FFRDC Rules of Behavior and obtain their supervisor's approval to gain access

[29] *See* U.S. Department of Homeland Security, Management Directive 262-05, Information Sharing and Safeguarding, *available at* https://www.dhs.gov/sites/default/files/publications/mgmt/information-and-technology-management/mgmt-dir_262-05-information-sharing-and-safeguarding.pdf.

to the system. Further, all FFRDC IT Enclave users are required to complete Privacy and Information Technology Security Awareness Training and adhere to DHS policies and directives when accessing the system. A privacy policy and security statement also appear on each FFRDC IT Enclave login screen reminding the user of the proper uses of the system. Punishments for failure to comply with these Rules of Behavior and training include a verbal or written warning, removal of system access, reassignment to other duties, criminal prosecution, civil liability, and/or termination of employment.

Privacy Risk: There is a risk that the FFRDC IT Enclaves will transfer information to a third-party environment (to another domestic or international server) and DHS will not be aware of the activity.

Mitigation: This risk is mitigated. The FFRDC IT Enclaves are closed environments; therefore, data will not enter or exit the security boundary on an automated and routine basis. Any additional interconnections (e.g., third party servers, systems) to the FFRDC IT Enclaves will be submitted through the Security Authorization Process, privacy review, and gain the required DHS approval before any data is transferred. In addition, DHS has authorized the following methods of data transport for the FFRDC IT Enclaves:

- Encrypted email and/or email with encrypted files;
- MITRE or RAND provided secure file transfer;
- Authorized DHS file transfer mechanism; and
- Other data transfer mechanism(s) approved by DHS S&T Office of the Chief Information Officer (OCIO) prior to use.

DHS information security staff will have access to the FFRDC IT Enclaves, to include system audit logs, to ensure data is being properly protected.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

While it is important for data used for research purposes to be accurate, relevant, timely, and complete, because this data is not used for operational decisions, it is not the paramount concern. However, FFRDCs have their own internal controls (e.g., a framework to protect against security breaches and preserve confidentiality, integrity, and availability) to ensure that data is accurate, relevant, timely, and complete, which are outlined in project specific contracts and Plans. Some data may come from other sources, such as DHS components, in which case, the FFRDCs rely on the entity providing the data for assurance of data quality and integrity. FFRDCs may also access commercial or open source data for research purposes, which FFRDCs ensure is accurate

when collected and used in accordance with appropriate research standards. The FFRDCs must adhere to the same guiding principles of public trust that the federal government does; therefore, the FFRDCs have implemented appropriate measures to ensure the data they collect and use is accurate.

Privacy Risk: There is a risk of inaccurate data being used in FFRDC activities.

Mitigation: This risk is partially mitigated. The contract and Technical Evaluation Plan for each FFRDC project will outline specific data requirements, to include purpose, use, and retention of data. However, because FFRDC uses of data for research purposes does not require the data to be accurate, relevant, timely, and complete as for operational data, this risk is not fully mitigated. The FFRDC does not attempt to make, nor does it have authority to make, operational decisions. If a component decides to use FFRDCs' data for an operational purpose, the component is responsible for verifying the accuracy of the data through its own processes.

The FFRDCs generally rely on data from other sources (e.g., DHS components, other federal, state and local government agencies, industry, academia, commercial vendors, and open source platforms); as such, the FFRDCs rely on the source entity for data accuracy and integrity. However, the FFRDCs, in collaboration with the FFRDC-PMO and the relevant DHS component privacy office, exercise due diligence during privacy reviews in evaluating the accuracy and relevance of any data used to ensure the research effort's soundness and the integrity of the research results.

Privacy Risk: There is a risk poor data quality may impact the output and or outcome of an FFRDC activity.

Mitigation: This risk is partially mitigated. The Homeland Security Systems Engineering Development Institute and the Homeland Security Operational Analysis Center FFRDCs are transitioning from a fragmented IT infrastructure to centralized DHS-accredited IT Enclaves and systems, which will standardize data protections and minimize the opportunity for poor data gathering, handling, and protocols. This transition will commence upon the publication of this PIA and completion of the DHS accreditation process. A significant portion of the FFRDCs' data will be derived from trusted data sources and will be migrated/integrated through DHS approved methods, such as encrypted email and/or emails with encrypted files, secure file transfers, or authorized DHS file transfer mechanisms.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

To support FFRDC activities, the FFRDCs are developing a contractually mandated technical environment for processing and storing current and future DHS data. The FFRDCs will transition to this technical environment (i.e., the FFRDC IT Enclaves) upon publication of this PIA and completion of the DHS accreditation process. This will allow DHS security and privacy controls to be applied to the system. This environment will be the primary IT resource for executing Homeland Security Systems Engineering Development Institute and Homeland Security Operational Analysis Center projects that collect, maintain, use, or store data. Each DHS-accredited IT Enclave will be further detailed in specific Addenda to this PIA.

The IT Enclaves will be used for a number of Homeland Security Systems Engineering and Development Institute and Homeland Security Operational Analysis Center projects supporting different DHS components, which may involve DHS data ---- including Unclassified, Controlled Unclassified Information, Sensitive but Unclassified (SBU), For Official Use Only (FOUO), PII, SPII, Law Enforcement Sensitive (LES), Protected Critical Infrastructure Information (PCII), and System Security Information (SSI).

Access to the IT Enclaves are limited to those with an authorized need to know within the FFRDCs. This need to know is determined by the individual's current job functions. Users may have access to the information if they have a legitimate need to know and based on job duties as validated by their supervisor and the system owner and have successfully completed all training requirements.

Privacy Risk: There is a risk of unauthorized loss or disclosure of PII during a data transfer.

Mitigation: This risk is partially mitigated. For access to the FFRDC IT Enclaves, administrators will ensure that adequate access controls are in place and maintained on all IT devices connected to the systems. The IT Enclaves are closed (and separate) environments; therefore, data will not enter or exit the security boundaries on an automated and routine basis. These security controls are captured in the respective Homeland Security Systems Engineering Development Institute and Homeland Security Operational Analysis Center IT Enclave System Security Plans (SSP). The SSP addresses how DHS conducts regular review of how data is maintained and any connections to external non-DHS systems.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

All DHS employees and contractors must complete annual training (e.g., Privacy, IT Security Awareness, and Records Management) to be provisioned into FFRDC systems and the FFRDC-PMO system to view the records based on their official need to know. User access and

activities are audited, with audit logs that capture the date, time, and search terms. Misuse may subject the user to disciplinary consequences in accordance with DHS policy, as well as criminal and civil penalties.

Access to information collected for specific projects will be outlined in project specific PTAs and the Technical Evaluation Plan for that project. Only individuals with a need to know will have access to the information collected for each project. The Homeland Security Systems Engineering and Development Institute and the Homeland Security Operational Analysis Center IT Enclaves, where DHS sensitive information for each project will be stored, implement audit controls to validate that DHS sensitive information are used, shared, disclosed, retained, and deleted in accordance with DHS legal and policy authorities.

Privacy Risk: There is a risk that DHS will not be able to audit or account for privacy-sensitive information maintained in the Homeland Security Systems Engineering and Development Institute and Homeland Security Operational Analysis Center IT Enclaves.

Mitigation: This risk is mitigated. DHS has several administrative controls that allow for accountability such as: (1) security reviews for IT Enclaves; (2) privacy compliance reviews for each Technical Evaluation Plan, regardless where the information is maintained; (3) FFRDC-PMO Quarterly Reviews; (4) this PIA has addenda to account for the types of FFRDC projects. The SSP addresses how DHS conducts regular review on how data is maintained and any connections to external non-DHS systems.

Privacy Risk: There is a risk that the FFRDCs may not respond appropriately to a privacy incident, such as unauthorized access or inappropriate disclosure of PII, which would impact the federal government's ability to render a timely mitigation strategy.

Mitigation: This risk is mitigated. DHS employees and contractors (cleared and authorized employees and sub-contractor personnel) are annually trained on Information Security and Privacy Incident Response policies and procedures for reporting and handling incidents to ensure that there is a consistent and appropriate response to incidents. The overall purpose of the training is to protect the confidentiality, integrity, and availability of FFRDC IT Enclave information systems and data in the event of a security incident.

Privacy Risk: There is a risk that the FFRDC will perform work for non-DHS projects, and these projects will not undergo privacy reviews similar to those required by DHS.

Mitigation: This risk is mitigated. The FFRDCs may perform work for others after the completion of an appropriateness review and obtaining funding through an interagency agreement. The FFRDCs are required to keep non-DHS activities separate from work for DHS but the FFRDC IT Enclaves are contractor owned and operated systems, and those capabilities can be contractually leveraged by non-DHS organizations (albeit through engagement with the FFRDC-PMO). Though

the FFRDCs may support and process information from non-DHS organizations, DHS data will have physical and logical separation and will not be comingled with any other data.

Conclusion

Homeland Security Systems Engineering and Development Institute and Homeland Security Operational Analysis Center are DHS-sponsored FFRDCs that deliver resources for specialized support services. The FFRDCs are not-for-profit organizations that are contractually overseen by the S&T FFRDC-PMO for contract execution and compliance with DHS policies/procedures.

As directed by DHS S&T, the FFRDCs are deploying DHS-accredited IT enclaves, which will be owned and operated by the contracting companies. The purpose of these technical environments is to enable the FFRDCs to execute project-specific task orders, which will involve DHS sensitive information, in furtherance of the homeland security enterprise mission. Through coordination with DHS component privacy offices, all FFRDC applicable data collections are handled in accordance with the Privacy Act to protect individual privacy and ensure mitigation of significant risks.

Contact Official

Maria Petrakis
Privacy Officer
Science & Technology Directorate

Responsible Official

Robert Burns
Executive Director
Office of Innovation & Collaboration
Science & Technology Directorate

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

ADDENDUM

Homeland Security Systems Engineering Development Institute (HSSEDI) IT Enclave Programs, Projects and Activities

The Homeland Security Systems Engineering and Development Institute IT Enclave uses both a physical and cloud-based computing environment (to include infrastructure, platform, security boundaries, applications, and services) that will support Homeland Security Systems Engineering and Development Institute projects and activities. The Homeland Security Systems Engineering and Development Institute IT Enclave infrastructure will be hosted primarily in the FedRAMP-approved Microsoft Azure for Government environments under documented approval and sponsorship from DHS S&T. The Homeland Security Systems Engineering and Development Institute IT Enclave resources (e.g., major applications or subsystems) hosted within Azure will also have access to dedicated Homeland Security Systems Engineering and Development Institute hardware through a private Multiprotocol Label Switching (MPLS) network at a MITRE location.

In the context of the Homeland Security Systems Engineering and Development Institute IT Enclave, Microsoft is an Infrastructure-as-a-Service (IaaS) and IaaS cloud provider. Microsoft provides the underlying FedRAMP authorized infrastructure that Homeland Security Systems Engineering and Development Institute IT Enclave Administrators use to provision IT components.

The Homeland Security Systems Engineering and Development Institute IT Enclave will be operated by MITRE; however, the S&T Office of the Chief Information Officer will support and perform technical oversight, to include:

1. Approving all gate reviews for Security Control Implementation(s);

2. Accessing the Homeland Security Systems Engineering and Development Institute IT Enclave to audit and scan for vulnerabilities and review system security logs;

3. Reviewing and approving all interconnection security agreements (ISA) between the Homeland Security Systems Engineering and Development Institute IT Enclave and resources outside the security boundary prior to operationalizing interconnections; and

4. Providing general implementation strategies aligned with the DHS 4300A, Sensitive Systems Handbook, to safeguard against threats.

In addition, the S&T Privacy Office will conduct audit reviews, as warranted, to support the Homeland Security Systems Engineering and Development Institute's ability to comply with privacy compliance requirements and to validate that privacy sensitive technologies, sensitive information, such as PII and other DHS sensitive information, are used, shared, disclosed,

retained, and deleted in accordance with DHS policy.

Prior to deployment of the IT Enclave, the S&T Privacy Office will deliver mandatory privacy training to all Homeland Security Systems Engineering and Development Institute staff and IT Enclave administrators. This training will cover data handling, user responsibilities, and articulate the issues raised in this PIA.

Data Collection

Data collections associated with the Homeland Security Systems Engineering and Development Institute IT Enclave are managed as separate storage volumes that require credentialed access to enable data use for each of the user roles defined—at a minimum access is granted, logged, and reviewed at the file level to administrator, project group, and individual levels. For each Homeland Security Systems Engineering and Development Institute-authorized project, DHS component program managers will coordinate with the appropriate DHS component privacy office to ensure that the Homeland Security Systems Engineering and Development Institute IT Enclave only collects, maintains, and uses data consistent with the purpose and routine uses of the DHS applicable guidelines, including respective component SORNs used by data owners for the original data collection.

DHS Sensitive Information

The Homeland Security Systems Engineering and Development Institute IT Enclave may process DHS sensitive information, which includes Unclassified, Controlled Unclassified Information (CUI), Sensitive but Unclassified (SBU), For Official Use Only (FOUO), Personally Identifiable Information (PII), Law Enforcement Sensitive (LES), Protected Critical Infrastructure Information (PCII), and Sensitive Security Information (SSI). In addition, personally identifiable information may contain sensitive information, including but not limited to, Social Security number, A-Number, medical history, and immigration status, depending on the specific project.

Homeland Security Systems Engineering and Development Institute projects may access a PII data set, some of which may contain sensitive information as an integral part of project task execution. These projects may have distinct privacy requirements surrounding the use, disclosure, retention, and destruction of the PII, as defined by the DHS/Sponsoring organization in the Homeland Security Systems Engineering and Development Institute Task Order. Homeland Security Systems Engineering and Development Institute projects obtain PII data sets from an external party, such as the sponsoring organization or publicly available data collections. These data collections will be assessed separately by the appropriate DHS Component privacy office.

Commercial Data

Homeland Security Systems Engineering and Development Institute has access and/or subscriptions to various commercial data sources, which may be (a) Publicly Available Data, data in the public domain that can be obtained or accessed from publicly accessible sources, both public and private; and (b) Public Record Data, data collected and maintained by a government entity for a public purpose and used outside of that public purpose. However, Homeland Security Systems Engineering and Development Institute is not permitted to use any commercial data for DHS projects or activities without explicit written approval from the FFRDC-PMO, Federal Project Leader, and the appropriate DHS component privacy office. The FFRDC-PMO, in consultation with the DHS component privacy office, will control FFRDCs commercial data use, in support of DHS activities, by implementing several controls (e.g., IDIQ, TEPs, IGCE, FFRDC Ordering Guide, Component Program Managers' Training).

Homeland Security Systems Engineering and Development Institute Projects

The Homeland Security Systems Engineering and Development Institute is required to leverage its the IT Enclave and/or an approved DHS environment for performing projects on behalf of DHS. To that end, there has been a data onboarding process established for new projects and the one-time migration of existing projects from another environment (e.g., MITRE network, DHS networks) into the Homeland Security Systems Engineering and Development Institute IT Enclave. The criteria for evaluating a project's candidacy comprises a combination of business, operational, and data sensitivity factors, as well as additional DHS/Sponsor requirements, such as security, privacy, and technical. Homeland Security Systems Engineering and Development Institute will develop an IT Enclave Project Migration Plan for submission to government oversight (e.g., FFRDC-PMO, component program managers, contracting officer representatives, appropriate DHS component privacy office) for final determinations as to whether projects will be permitted to migrate, and if so, how. The list in the Homeland Security Systems Engineering and Development Institute IT Enclave Migration Plan and respective Project Management Plans will be updated to reflect the final disposition of candidate projects.

As projects are defined for the different DHS components or other federal, state local, and tribal government entities, through engagement with the FFRDC-PMO, there may be other data types that are required for task order execution. All Homeland Security Systems Engineering and Development Institute project activities will require a privacy review from the appropriate DHS component privacy office, which may include a project-level PTA that will detail specific data elements. Some Homeland Security Systems Engineering and Development Institute projects involve classified information; however, the Homeland Security Systems Engineering and Development Institute IT Enclave is not authorized to process classified information. Those security sensitive projects will remain on other DHS approved systems.