OFFICE OF INSPECTOR GENERAL

S&T Needs to Improve Its Management and Oversight of R&D Projects

Homeland Security

March 7, 2022

OIG-22-30

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

March 7, 2022

MEMORANDUM FOR: Kathryn Coulter Mitchell
Senior Official Performing the
Duties of the Under Secretary
Science and Technology Directorate

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI Digitally signed by JOSEPH V CUFFARI Date: 2022.03.05 10:31:57 -05'00'

SUBJECT: *S&T Needs to Improve Its Management and Oversight of R&D Projects*

Attached for your action is our final report, *S&T Needs to Improve Its Management and Oversight of R&D Projects*. We incorporated the formal comments provided by your office.

The report contains five recommendations aimed at improving execution of the Science and Technology Directorate research and development projects. Your office concurred with all five recommendations. Based on information provided in your response to the draft report, we consider recommendations 3 and 4 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Based on information provided in your response to the draft report, we consider recommendations 1, 2, and 5 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to, OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and

appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG Highlights

S&T Needs to Improve Its Management and Oversight of R&D Projects

March 7, 2022

Why We Did This Audit

S&T aims to deliver timely, innovative technology solutions to bolster DHS mission operations. To do this, S&T works with DHS and its components to identify capability gaps in DHS operations and to research and develop technologies to address those gaps. We conducted this audit to determine whether S&T executes R&D projects in accordance with Federal and DHS guidelines, policies, and procedures.

What We Recommend

We made five recommendations to S&T to improve the execution of R&D projects.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Department of Homeland Security Science and Technology Directorate (S&T) did not execute all research and development (R&D) projects in accordance with Federal and DHS guidelines, policies, and procedures. Specifically, S&T did not consistently comply with sensitive information and privacy requirements to protect sensitive information. In addition, not all S&T project managers obtained the required Federal Acquisition Certification to ensure they met training, experience, and development requirements. Finally, for most R&D projects we reviewed, S&T project managers did not prepare project plans for review and approval.

We attribute S&T's noncompliance to insufficient oversight and guidance to ensure necessary steps were completed for each project. S&T also does not have a centralized approach to manage and monitor project execution, further hindering its ability to ensure compliance.

Without effective management and monitoring of R&D projects, S&T faces increased risk of unauthorized disclosure of sensitive and personally identifiable information. It also faces greater risk of projects missing milestones, exceeding the budget, or not achieving desired objectives. As a result, S&T may not be able to fully achieve its mission to research and develop technologies addressing gaps in DHS operations.

S&T Response

S&T concurred with all five recommendations. We included a copy of S&T's comments in Appendix B.

Table of Contents

Abbreviations

EPIC	Execution, Performance, Invoice, Consolidation
FAC-P/PM	Federal Acquisition Certification for Program and Project Managers
GAO	Government Accountability Office
MCS	Office of Mission and Capability Support
OES	Office of Enterprise Services
OIC	Office of Innovation and Collaboration
OMB	Office of Management and Budget
OSE	Office of Science and Engineering
PII	personally identifiable information
PTA	Privacy Threshold Analysis
R&D	research and development
S&T	Science and Technology Directorate
STATS	Science and Technology Analytical Tracking System

Background

Federal agencies must continually identify ways to apply new and emerging technologies to improve how they carry out mission operations and deliver services for the American people. The *Homeland Security Act of 2002*,[1] *as amended*, gives the Science and Technology Directorate (S&T) primary responsibility for research and development[2] (R&D) within the Department of Homeland Security. S&T provides DHS and its components, as well as state and local partners, with the technology and capabilities needed to protect the homeland. Specifically, S&T R&D activities are meant to anticipate and respond to changes in technology and threats and to address unmet needs or gaps in existing DHS technology capabilities.

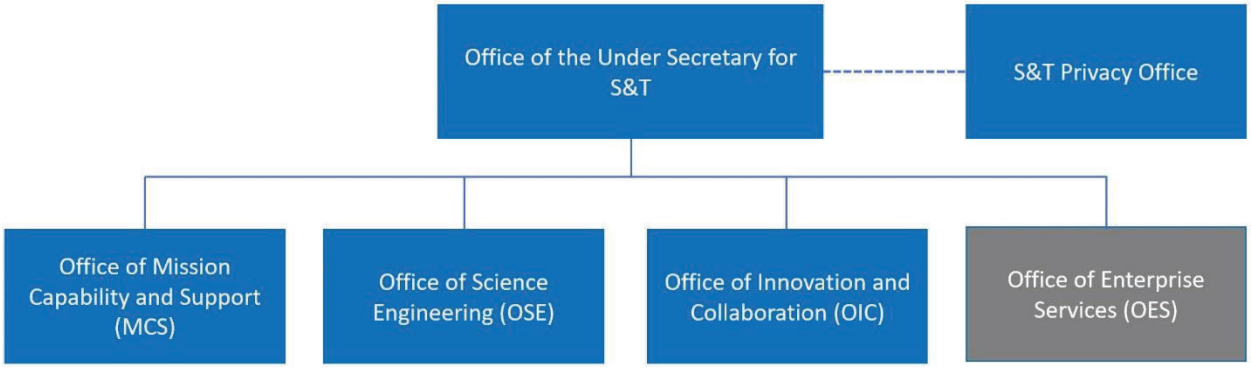
S&T's mission is to enable effective, efficient, and secure operations across all homeland security missions by applying scientific, engineering, analytic, and innovative approaches to deliver timely solutions and support departmental acquisitions. To accomplish its mission, S&T works with DHS and its components to identify capability gaps in DHS operations and to research and develop technologies to address those gaps. For example, to address the growing need for new or improved border surveillance capabilities, S&T initiated a Ground Based Technologies Program to focus R&D projects on enhancing situational awareness, providing automated detections and alerts, and enhancing the safety of DHS officers and agents. Similarly, to address the need for effective screening of air cargo, S&T initiated an Air Cargo Screening Program to develop new security technologies to cost-efficiently screen diverse and complex cargo. In fiscal year 2020, S&T budgeted $18.4 million for these two programs.

S&T Organization

S&T is composed of a Privacy Office and four operational offices that support DHS components and homeland security customers, as shown in Figure 1.

[1] *Homeland Security Act of 2002*, Pub. L. No. 107–296.
[2] R&D is a systematic study and application of knowledge aimed at discovering and producing solutions to meet an operational need.

Figure 1. S&T Organizational Chart



Source: DHS Office of Inspector General-created, based on S&T's organizational chart as of November 10, 2021

- The Privacy Office, within the Office of the Under Secretary, assesses the privacy risks in programs and systems within S&T, and develops privacy mitigation strategies. The mission of the S&T Privacy Office is to protect individuals by embedding and enforcing privacy protections and transparency in all S&T activities.

- MCS works with S&T customers throughout the R&D process to define priorities, gaps, and requirements and to find or develop technology solutions for the homeland security mission.

- OSE provides technical functions and services to S&T programs, DHS components, and other homeland security customers such as the Federal, state, and local first responder community, by conducting research to identify and understand current, emerging, and future threats, and offering subject matter expertise.

- OIC provides DHS access to technology-based capabilities and solutions through a network of partnerships with other Federal departments and agencies, industry and international partners, and academia. OIC manages tools and contract mechanisms that allow S&T to sponsor critical R&D activities.

- OES supports S&T operations, including the management of personnel, finance and budget, facilities, information technology, compliance, contract administration, and security. Within OES, the Program Support

Office provides direct support to program[3] and project[4] managers throughout S&T and facilitates the development of common standards, guidance, and program and project management processes for S&T.

S&T's R&D Business Process Flow

In 2018, S&T developed a set of high-level foundational processes, known as the Operating Model Blueprint, to standardize common program and project management practices for R&D efforts. In 2019, S&T formally documented its R&D Business Process Flow[5] to define the required steps and activities to ensure alignment with S&T's Operating Model Blueprint during R&D project execution. The process flow includes steps that outline how S&T executes projects. Some of these steps include:

- review the viable options and select an approach;
- assign a project manager;
- ensure a project manager identifies resources and forms the project team; and
- develop a project management plan (project plan).

According to the 2019 R&D Business Process Flow, the S&T project manager performs tasks in accordance with the project plan to develop and test a capability that meets the customer's requirement and to deliver the solution to the customer. The project manager is responsible for managing the solution development activities, including authorizing and directing work, verifying the work is completed, and implementing corrective actions, if necessary. Additionally, the project manager is responsible for monitoring and reporting project risks and issues, assessing progress, reporting status information, and communicating with stakeholders. When the project is executed as part of a program that encompasses multiple projects, the project manager works closely with the program manager to ensure project and program objectives align.

The project manager is also responsible for completing sensitive information compliance requirements. For example, the project manager is responsible for

[3] S&T defines a program as the "totality of activities directed to accomplish specific goals and objectives, which may provide new or improved capabilities in response to approved requirements and/or sustain existing capabilities, and which may have multiple projects to obtain specific capability requirements or capital assets."
[4] S&T defines a project as a "temporary endeavor undertaken to create a unique product, service, or result; involves the definition, acquisition, and fielding of a unique product, service or result in accordance with specified resources and requirements."
[5] *Understanding S&T's Business Process Flow*, *Overview of S&T's Research, Development and Matrixed Process*, Version 1, October 15, 2019.

submitting the Checklist for Sensitive Information and a Privacy Threshold Analysis (PTA) to the S&T Privacy Office for review. The checklist is designed to help the user create safeguards for sensitive information[6] by identifying whether contractors will have access to sensitive information and whether contractor information technologies will be used to input, store, process, output, and/or transmit sensitive information. In addition, a PTA includes a general description of the system or program and describes whether personally identifiable information[7] (PII) is collected, and if so, from whom, and how that information will be used.

Prior Reporting and Oversight

In March 2019, the Government Accountability Office (GAO) reported[8] that S&T used disparate information sources to identify and track R&D project information, leading to difficulty integrating complete R&D project information and resulting in reporting that was not comprehensive. GAO recommended that the Secretary of Homeland Security develop a mechanism to align processes and information sources for collecting R&D project data from DHS components to ensure information could be collected, integrated, and result in a comprehensive accounting of R&D projects DHS-wide. As of September 2021, GAO closed all the recommendations as implemented.

In March 2020, DHS OIG received allegations of potential privacy violations relating to project *Night Fury*, conducted by OSE, to research and develop open source data analytics tools. For this $443,000 project, S&T contracted specific tasks to a university to collect social media data on behalf of S&T. OSE sought to test and develop analytic capabilities to identify potential terrorism risks on publicly available social media and other open source platforms. The complainant stated the project began in September 2018 and specifically included data collection of millions of social media records, including posts, videos, and photos. Also, the complainant notified OIG of concerns that S&T may not have ensured effective programmatic oversight, employee accountability, Federal records management, contract documentation, and information security for this specific project.

---

[6] Sensitive information is any information, which if lost, misused, disclosed, or without authorization is accessed or modified could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the *Privacy Act of 1974*.

[7] Personally identifiable information is information that permits an individual's identity to be directly or indirectly inferred, including other information that is linked or linkable to an individual. For example, when linked to an individual, such information includes the person's name, social security number, date and place of birth, etc.

[8] *Research & Development Coordination Has Improved, but Additional Actions Needed to Track and Evaluate Projects*, GAO 19-210, March 2019.

During our review of this allegation, we identified privacy safeguards that should have been in place for this project, including a Checklist for Sensitive Information and a PTA. We reviewed project *Night Fury* and determined it did have a completed checklist and a PTA that was currently under review by the DHS Privacy Office. Based on this review, we conducted a broader review of 24 R&D projects. In FY 2020, S&T had 369 ongoing R&D projects in the execution phase, with obligations totaling $305 million[9] — an average obligation of $826,000 per project. We conducted this audit to determine whether S&T executes R&D projects in accordance with Federal and DHS guidelines, policies, and procedures.[10]

Results of Audit

S&T did not execute all R&D projects in accordance with Federal and DHS guidelines, policies, and procedures. Specifically, S&T did not consistently comply with sensitive information and privacy requirements to protect sensitive information. In addition, not all S&T project managers obtained the required Federal Acquisition Certification to ensure they met training, experience, and development requirements. Finally, for most R&D projects we reviewed, S&T project managers did not prepare project plans for review and approval.

We attribute S&T's noncompliance to insufficient oversight and guidance to ensure necessary steps were completed for each project. S&T also does not have a centralized approach to manage and monitor project execution, further hindering its ability to ensure compliance.

Without effective management and monitoring of R&D projects, S&T faces increased risk of unauthorized disclosure of sensitive and PII. It also faces greater risk of projects missing milestones, exceeding the budget, or not achieving desired objectives. As a result, S&T may not be able to fully achieve its mission to research and develop technologies addressing gaps in DHS operations.

[9] S&T provided the number and dollar amount of R&D projects in the execution phase during FY 2020. See the table in Appendix A for a detailed examination.
[10] See Appendix A for a description of our sample selection and testing methodology.

S&T Did Not Comply with All Sensitive Information and Privacy Requirements

Based on our review of S&T privacy safeguards for 24 R&D projects, we determined that S&T did not comply with sensitive information and privacy requirements for some projects. Although S&T project managers prepared the necessary Checklist for Sensitive Information documentation to account for sensitive information for most projects we reviewed, the contracts for some projects did not include the special clauses required to ensure protection of sensitive information. In addition, we determined that S&T did not prepare a PTA for all R&D projects as required.

S&T Did Not Comply with Checklist for Sensitive Information Requirements

The S&T Privacy Office assists the DHS Privacy Office with addressing privacy incidents and complaints within S&T. The S&T Privacy Officer's responsibilities include:

- maintaining ongoing review of all component information technology systems and programs, information sharing, and other activities to identify collections and uses of PII;
- coordinating with system and program managers to complete required privacy compliance documentation; and
- overseeing component implementation of DHS and component privacy policy, including procedures and guidance for handling suspected and confirmed privacy incidents.

The S&T Privacy Office is also responsible for ensuring compliance with Federal and DHS privacy policies and procedures. At the Federal level, the *Homeland Security Act of 2002*, *as amended*, requires the DHS Privacy Officer to establish privacy policies that ensure the use of technologies sustain and do not erode privacy protections. The S&T Privacy Office ensures this by completing privacy compliance documentation. At the Department level, the *DHS Acquisition Manual*[11] requires S&T to complete a Checklist for Sensitive Information for all project acquisitions, regardless of dollar value. The manual also requires review of the completed checklist by the Component Chief Information Officer, Chief Security Officer, and Privacy Officer, as well as other DHS officials in specific circumstances.

[11] *DHS Acquisition Manual*, *Security Requirements for Contractor Access to Unclassified Facilities, IT Recourses, and Sensitive Information,* 3004.470(b), October 2009.

As part of the completion of the Checklist for Sensitive Information, prior to funding the project, S&T officials determine whether an R&D project acquisition will have a high risk of unauthorized access to or disclosure of sensitive information. For example, S&T officials designated one project high-risk because the contractor would have access to videos, photos, and audio that may contain PII. When an R&D project is deemed high-risk, the contracting officer must include three special clauses in the contract:

1. Safeguarding of Sensitive Information;
2. Information Technology Security and Privacy Training; and
3. Contractor Employee Access.

These special clauses provide privacy and security protections, mandate privacy training for contractors, and hold contractors responsible in case of a PII breach. The clauses and associated language are to be added into the contract without revision.

For the 24 projects we reviewed for compliance with the Checklist for Sensitive Information requirements, including the addition of special clauses where applicable, project managers prepared the checklist for 22 (92 percent). However, 3 of the 22 checklists were not signed by the appropriate officials. In one of the three, the Chief Information Officer did not sign the checklist as required.[12] The second checklist was not signed by officials from the DHS Cybersecurity and Infrastructure Security Agency and the Transportation Security Administration, which were required because the contractor would have access to vulnerable and sensitive security information.[13] An official from the Transportation Security Administration did not sign the third checklist even though the project required review by that component because the contractor would have access to sensitive security information.

We also identified three instances in which the Checklist for Sensitive Information was signed by the appropriate official, indicating it was reviewed and approved, but the checklist was not filled out completely. Two were completed incorrectly, one of which indicated that contractor support was necessary to complete privacy compliance documentation but did not identify

[12] This signature was required because it was unclear whether contractor information systems would be used to input, store, process, output, or transmit sensitive information.
[13] Sensitive security information is information obtained or developed in the conduct of security activities, including R&D, upon which disclosure of this information would: (1) constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file); (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation.

and describe the activities and level of support needed. In the other instance, entire sections of the approved checklist were not completed.

Project managers did not prepare the Checklist for Sensitive Information for 2 of the 24 projects. These projects, with total obligations of almost $398,000, were part of an $8 million program for which a checklist was completed. This checklist indicated that the program would have a high risk of unauthorized access to or disclosure of sensitive information. Although a small percentage of the total program costs, we could not determine whether these two projects were at high risk of unauthorized access to or disclosure of sensitive information because the projects were not individually addressed in the checklist.

Although project managers completed the checklists for most projects we reviewed, the contracts for some high-risk projects did not contain the required special clauses. S&T officials determined that 12 of the 24 R&D projects we reviewed were high-risk. However, only 6 of the 12 contracts contained all three required special clauses. The contracts for the remaining six projects were missing at least one of the required special clauses. The contracts for three of the six R&D projects did not contain any of the three special clauses, as shown in Table 1.

Table 1. Required Special Clauses in Contracts for High-Risk Projects

	12 Projects Identified as High-Risk											
Special Clauses	1	2	3	4	5	6	7	8	9	10	11	12
Safeguarding of Sensitive Information	✓	✓	X	X	✓	✓	✓	✓	✓	✓	✓	X
Information Technology Security & Privacy Training	✓	✓	X	X	✓	✓	✓	✓	✓	✓	✓	X
Contractor Employee Access	✓	✓	X	X	✓	X	✓	✓	X	✓	X	X

✓Clause Included; X Clause Not Included
Source: DHS OIG prepared based on fieldwork results

The DHS Office of Procurement Operations provides S&T with procurement and acquisition management services. According to an Office of Procurement Operations official, the required special clauses were not included in the contracts for the six high-risk projects due to contracting officer error. To remedy this oversight, the office planned to incorporate the missing special clauses through modifications to the contract documents. Without the special clauses included in the contract, S&T is at increased risk of unauthorized disclosure of sensitive information, which could result in privacy incidents involving PII.

Project Managers Did Not Prepare a Privacy Threshold Analysis for All Projects

DHS privacy policy[14] requires that project managers, in consultation with the Component Privacy Officer, complete a PTA for all R&D projects. The PTA must be provided to the DHS Privacy Office for review. The DHS Privacy Office uses a PTA to identify programs, projects, and systems that are privacy sensitive and to assess the need for further privacy compliance documentation.

S&T project managers did not prepare a PTA for 13 (54 percent) of the 24 projects reviewed, even though the checklist indicated that 9 of the 13 projects involved PII. Additionally, two project managers prepared PTAs for the program instead of the project. However, the program PTAs did not address how the specific projects within the program would manage PII.

S&T project managers completed PTAs for 9 of 24 projects, but at the time of our audit, the DHS Privacy Office had not yet reviewed and approved two of the nine completed PTAs, and a third completed PTA was still under review by the S&T Privacy Office. However, S&T began executing these three projects before the privacy compliance process was completed. For three of the six PTAs that were completed, reviewed, and approved, the DHS Privacy Office had determined the projects needed additional privacy documentation, which the project manager prepared as required.

During our review of the checklists for the 24 projects, we identified 10 instances in which the S&T Privacy Office requested (on the checklist) that the project manager complete a PTA. In one instance, the S&T Privacy Office explicitly requested a PTA for a high-risk project, but the project manager did not prepare one, asserting that a PTA was not required for the project and that the S&T Privacy Office had already reviewed the checklist.

In 2019, the DHS Privacy Office completed a Privacy Compliance Review[15] of S&T's privacy compliance process. The office reported that S&T had historically produced minimal privacy compliance documentation even though its R&D projects included PII. It also reported that S&T had not followed the prescribed PTA process. According to the DHS Privacy Office, preparation of the PTA and review by the Privacy Office are not optional, and S&T is not authorized to determine whether a project is privacy sensitive, even for projects the program manager deems as not impacting privacy. The DHS Privacy Office also reported that S&T did not submit documentation for several major projects

[14] DHS Instruction, 140-06-001, *Privacy Policy for Research Programs and Projects,* August 2012.
[15] *Privacy Compliance Review of the Science and Technology Directorate*, June 24, 2019.

until the projects were ready to start, which allowed no time to fully adjudicate privacy concerns.

Additionally, the DHS Privacy Office noted in its report that, with increased S&T Privacy Office staffing, the quality and timeliness of privacy compliance documentation had improved. However, for six projects we reviewed for which PTAs were not completed, the contracts were executed after the DHS Privacy Office issued its report to S&T.

Without a PTA, S&T and DHS cannot identify projects that are privacy sensitive. They also cannot demonstrate the inclusion of privacy considerations during the review of the project, demonstrate compliance with privacy laws and regulations and, for projects the DHS Privacy Office determines are privacy-sensitive, identify and mitigate privacy risks. Without a PTA, the S&T Privacy Office does not have insight on privacy matters within those projects. For example, the PTA associated with the hotline complaint required additional privacy compliance documentation. When the S&T Privacy Office staff began creating the documentation, they had concerns about privacy matters with the project and elevated the concerns to the DHS Privacy Office. Without a PTA, this level of oversight would not have happened.

Not All R&D Project Managers Obtained the Federal Acquisition Certification for Program and Project Managers

We also sought to determine compliance with appropriate Federal acquisition certification requirements. Office of Management and Budget (OMB)[16] and DHS policy[17] require all program and project managers to obtain Federal Acquisition Certification for Program and Project Managers (FAC-P/PM). Project managers are critical for developing Government requirements, defining measurable performance standards, and managing lifecycle activities to ensure that intended outcomes are achieved. The FAC-P/PM establishes general training, experience, and development requirements for program and project managers.

The FAC-P/PM contains three levels of certification: entry-, mid-, and senior-level. The appropriate level of certification needed to lead a program or project is determined by the agency. DHS policy states that entry-level certification is appropriate for project team members, mid-level certification is appropriate for

[16] OMB Memorandum for Chief Acquisition Officers, Senior Procurement Executives, *Revisions to the Federal Acquisition Certification for Program and Project Managers (FAC-P/PM),* December 16, 2013.
[17] DHS Policy 064-04-001, *Acquisition Certification Requirements for Program and Project Management*, April 2014.

project managers and those managing programs of low to moderate risk, and senior-level certification is appropriate for personnel who manage and evaluate moderate to high-risk programs. OMB requirements and DHS policy allow project managers to meet the certification requirements within 12 months of their assignment to a project.

Of the 24 projects we reviewed, S&T project managers for 9 of them had obtained the appropriate FAC-P/PM certification, and one additional project manager was in the process of obtaining the certification. However, project managers for the remaining 14 projects were not FAC-P/PM-certified. Of the 14 projects managed without a FAC-P/PM-certified project manager, 4 were identified as high-risk for sensitive information on the project's checklist.

Although not FAC-P/PM-certified, 8 of the 14 project managers had Contracting Officer's Representative certifications, and two project managers had Program Manager certifications issued by external organizations. OMB requirements state that an individual with a Contracting Officer's Representative certification does not necessarily meet the requirements for the FAC-P/PM. In addition, DHS policy allows current DHS Program Manager certifications to be converted to FAC-P/PM, but to do so, personnel certified in program management or holding other external certifications must meet additional requirements.

S&T did not require R&D project managers to obtain the FAC-P/PM certification. Although, in an October 2019 memorandum to S&T management, the Program Support Office recommended that all S&T project managers be FAC-P/PM-certified, only one of the three S&T offices, MCS, required its project managers to obtain the certification. However, project managers for 7 of the 15 MCS projects we reviewed were not certified.

An S&T official stated that R&D project managers were exempt from the certification because research projects are not considered acquisition projects. However, OMB guidance states that the *Services Acquisition Reform Act of 2003*[18] expanded the definition of acquisition to include functions performed by program and project managers. Further, the guidance states that the certification is mandatory for project managers who are responsible for, among other things, accomplishing a specifically designated work effort established to achieve stated objectives, defined tasks, or other units of related effort on a schedule, within cost constraints and in support of the program mission or objective. In addition, the guidance states that waivers of certifications are not allowed.

[18] *The Services Acquisition Reform Act of 2003*, P.L. 108-136.

Without FAC-P/PM certification, S&T project managers may not gain the necessary knowledge and skills to manage R&D projects, particularly those that are high-risk, high-impact. Establishing FAC-P/PM requirements for this critical workforce will better position S&T for success in its R&D efforts.

Project Managers Did Not Prepare a Project Plan for All R&D Projects

Lastly, we sought to determine compliance with S&T's project management requirements, as defined in its 2019 R&D Business Process Flow. The documented process flow states project managers are required to prepare a project plan for all MCS projects, while S&T management must review and approve the plan before the project execution begins.[19] The project plan establishes the total scope of work, defines project objectives, and develops the course of action to meet those objectives.

We determined S&T project managers did not prepare project plans for most (92 percent) of the 24 R&D projects we reviewed. Specifically, project managers prepared project plans for only 2 of the 24 projects. Although the two plans included the required information, the plans were not approved by S&T management before the project execution phase, as required. For the remaining 22 projects, project managers did not prepare project plans. Instead of project plans, project managers prepared program plans for 16 projects, research plans for 2 projects, and no plans for 4 projects.

Without a project plan, project managers' ability to track the completion of project tasks and oversee contractor performance and deliverables may be hindered. This could result in increased risk of projects missing milestones or exceeding the budget. Additionally, project managers may not anticipate and mitigate project risks and issues that could prevent the project from achieving the desired objective.

S&T Did Not Sufficiently Manage and Monitor R&D Project Execution

S&T did not have sufficient guidance or oversight to ensure compliance with Federal and DHS guidelines, policies, and procedures when executing R&D projects. In addition, S&T did not have a centralized system to manage and monitor R&D projects.

[19] Although S&T is only applying the process flow to MCS-based programs and projects, OIC and OSE officials stated that their project managers must also prepare project plans for the projects they manage.

S&T Did Not Have Sufficient Oversight or Guidance for Project Execution

S&T project managers did not comply with all sensitive information and privacy requirements due to a lack of oversight to ensure necessary steps were completed. For example, although the contracting officers are supposed to include the special clauses in the contracts for high-risk projects, S&T project managers did not consistently review the documents to ensure the special clauses were inserted. Instead, according to an S&T official, providing the contract to the project manager for review varies depending on the contracting officer. Additionally, project managers may focus their review on the specific project requirements of the contract rather than the special clauses. Finally, S&T has not clearly communicated the requirement to prepare a PTA to ensure project managers prepare them. Project managers stated that they did not prepare a PTA because they were not aware that a PTA was required or believed that a PTA was only required if the project collected PII.

Although the 2019 Business Process Flow's applicability is limited to MCS-based programs and projects, S&T did not provide project managers in S&T with clear and sufficient guidance for executing R&D projects. An S&T official stated the Business Process Flow was the only S&T guidance for R&D project managers. In addition, although the Project Management Plan Template[20] states that the project plan is meant to be tailored to the needs of the project based on size, complexity, and duration, the Business Process Flow does not clearly state the difference, if any, in the requirements to prepare project plans, as well as checklists and PTAs, for standalone projects and projects performed as part of larger programs. The process flow also does not directly address the requirements, form, and minimum content for project plans for research projects. The limited application of the Business Process Flow to MCS and its lack of detailed guidance resulted in confusion and differing interpretations of when checklists, PTAs, and project plans were required for projects.

The Business Process Flow references additional guidance from the 2019 *Program and Project Manager Handbook.*[21] However, S&T had not finalized and implemented the handbook at the time of this audit. In addition, during our audit, S&T released an updated 2021 version of the Business Process Flow.[22] The 2021 version applies to programs and projects in all S&T offices, but it

[20] The Program Support Office developed a Project Management Plan Template for R&D project managers in 2019. The template instructions indicate that project managers can tailor the plan to fit the specific needs of each project.
[21] *Program & Project Management Handbook, A Reference for Program and Project Management in the Science and Technology Directorate*, Version 0.1, July 30, 2019.
[22] *Understanding S&T's Business Process Flow, Overview of S&T's Matrixed Research and Development Process*, Version 2, March 11, 2021.

does not clearly address how to apply the requirements to different types of projects.

S&T Did Not Have a Centralized Approach to Manage and Monitor R&D Projects

S&T has not yet implemented a centralized approach to manage and monitor R&D project execution. Instead, S&T relied on multiple information technology systems that were neither integrated nor intended for project management purposes. For example, to provide us with information on its projects, S&T used Execution, Performance, Invoice, Consolidation (EPIC), a legacy system that pulls information from the Federal Financial Management System.[23] However, S&T was unable to provide the project status of all R&D projects. To satisfy our request for a list of projects executed during FY 2020, S&T obtained a list of R&D projects with obligations from EPIC. To obtain a list of project managers for the 24 projects we selected for review, S&T pulled the information from a second system — the Procurement Request Information System Management, but 14 of the 24 (58 percent) project managers were inaccurate.

S&T's management of project records is decentralized, which prevented efficient data gathering for this audit. Instead, S&T relied on individual project managers to maintain their own records of official project files and documentation for each project they manage. This proved challenging when project managers were out of the office or no longer worked for S&T. In addition, when S&T officials needed project information, S&T sent a data request out to all program and project managers. For example, in February 2020, an S&T official emailed all S&T offices requesting that they each provide all project plans or other relevant project documentation as well as a list of all S&T program and project managers.

S&T began transitioning from EPIC to its replacement system — the Science and Technology Analytical Tracking System (STATS) — in August 2018. STATS can track projects and store privacy and project documentation, and it includes risk and workforce management tools. For example, according to the STATS user guide, STATS can generate information about cost, schedule, quality, risk, and customer satisfaction, which project managers can use for status updates to management and to the customer. During our audit, in May 2021, STATS received its official system designation and EPIC was decommissioned in August 2021. Although S&T encouraged project managers to use STATS, at the time of our audit, S&T had not yet mandated the use of STATS across all S&T offices. Without a centralized system enabling

[23] The Federal Financial Management System is a web-based, workflow management and financial transaction system that provides core financial management functions for S&T.

management to readily obtain the information necessary to track and monitor R&D projects, S&T cannot ensure compliance with Federal and DHS guidelines, policies, and procedures.

Conclusion

Without effective oversight of its compliance with privacy protections, S&T may be at risk of inadvertently disclosing sensitive information or PII. For example, when R&D projects are initiated without special clauses for sensitive information and PTAs, the risk of unauthorized disclosure of sensitive information increases and is more vulnerable to privacy incidents involving PII. Likewise, without effective project management and monitoring practices, S&T may not be able to achieve its mission to deliver timely solutions and support departmental acquisitions. Until S&T improves its management and monitoring of R&D project execution, it will be at risk of not meeting its mission to research and develop technologies addressing gaps in DHS operations.

Recommendations

Recommendation 1: We recommend the Senior Official Performing the Duties of the Under Secretary for the Science and Technology Directorate, in consultation with the Office of Procurement Operations, develop and implement a process to ensure required special clauses are included in contracts for project acquisitions with a high risk of unauthorized access to or disclosure of sensitive information.

Recommendation 2: We recommend the Senior Official Performing the Duties of the Under Secretary for the Science and Technology Directorate develop and implement a process, with a timeline, to ensure that project managers prepare Privacy Threshold Analyses for all projects and provide the analyses to the S&T Privacy Office for review.

Recommendation 3: We recommend the Senior Official Performing the Duties of the Under Secretary for the Science and Technology Directorate clarify the requirements for the preparation of Checklists for Sensitive Information, Privacy Threshold Analyses, project plans, update S&T guidance, and formally communicate the requirements to program and project managers.

Recommendation 4: We recommend the Senior Official Performing the Duties of the Under Secretary for the Science and Technology Directorate develop and implement a policy to require and track FAC-P/PM certification for research and development program and project managers that meets Office of Management and Budget and Department of Homeland Security requirements.

Recommendation 5: We recommend the Senior Official Performing the Duties of the Under Secretary for the Science and Technology Directorate require that program and project managers use the Science and Technology Analytical Tracking System, or other centralized project management system, to track and manage all research and development projects.

S&T Comments and OIG Analysis

We obtained written comments on a draft of this report from S&T. We have reviewed S&T's comments, as well as the technical comments previously submitted under separate cover, and updated the report as appropriate. S&T concurred with all five recommendations. A summary of S&T's responses and our analysis follows.

S&T's Comments to Recommendation 1: Concur. The S&T Compliance Division and the S&T Office of Contracts, Acquisition, and Program Support are collaboratively drafting a formal process, and associated implementation training, in consultation with the Office of Procurement Operations, to ensure the proper clauses are included in contracts for project acquisitions with a high risk of unauthorized access to, or disclosure of, sensitive information. Once complete, this formal process and training will be provided to Program Managers, Contract Officer Representatives, and staff in the S&T Compliance Division.

Additionally, in July 2021, a "Project Situational Compliance" Checklist was added as Appendix A to the current S&T internal Program and Project Management Plan templates, which requires PMs to consider all compliance requirements impacting their program prior to the Procurement Request submission. Estimated Completion Date (ECD): January 31, 2023.

OIG Analysis of S&T's Comments: S&T's actions are responsive to this recommendation, which will remain open and resolved until S&T provides documentation showing that all planned corrective actions are completed.

S&T's Comments to Recommendation 2: Concur. The S&T Compliance Director, in coordination with leadership across the Directorate and the S&T Program Support Office, is developing a process with associated timeline, checklists, and guidance to ensure that the privacy documentation, including the projected timeline with milestones, is developed, as appropriate. Once complete, this process will be formally communicated to program and project managers to ensure the requirements are understood. ECD: January 31, 2023.

OIG Analysis of S&T's Comments: S&T's actions are responsive to this recommendation, which will remain open and resolved until S&T provides documentation showing that all planned corrective actions are completed.

S&T's Comments to Recommendation 3: Concur. The S&T Compliance Director is leading the effort to develop a process, including projected timelines and milestones, to clarify the requirements of privacy documentation. Once complete, this process will be formally communicated to program and project managers to ensure the requirements are understood. ECD: January 31, 2023.

OIG Analysis of S&T's Comments: S&T's actions are partially responsive to this recommendation. However, the corrective action does not address additional guidance for project plans. The recommendation will remain open and unresolved until S&T provides documentation showing that all planned corrective actions, including guidance for project plans are completed.

S&T's Comments to Recommendation 4: Concur. On December 1, 2021, the Director of Mission Capability Support issued a memorandum, "Federal Acquisition Certification for the Office of Mission and Capability Support (MCS) Program Managers (FAC-P/PM) Certification," requiring project management certifications for all program managers. The Program Support Office is coordinating with the Human Capital Office and S&T Principal Directors to enhance existing processes to also track PM certifications.

Additionally, OMB is currently rolling out the Competency Exploration for Development and Readiness tool, in coordination with the DHS Office of the Chief Human Capital Officer (OCHCO), during 2022. The Program Support Office is working with OCHCO and the Principal Directors to begin using this tool within S&T, which will collect data to baseline project management capabilities within the organization and identify areas where S&T needs to increase certifications and skills to appropriate levels. ECD: March 31, 2023.

OIG Analysis of S&T's Comments: S&T's actions are partially responsive to this recommendation. However, programs and projects are also being executed in OIC and OSE. Therefore, this recommendation will remain open and unresolved until S&T provides documentation showing the FAC P/PM is applied to all program and project managers conducting R&D.

S&T's Comments to Recommendation 5: Concur. STATS is the current authoritative data source for all research and development projects. The Deputy Under Secretary for S&T will issue a formal memorandum requiring the use of STATS for all research and development projects. ECD: March 31, 2022.

OIG Analysis of S&T's Comments: S&T's actions are responsive to this recommendation, which will remain open and resolved until S&T provides documentation showing that all planned corrective actions are completed.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*. Our audit objective was to determine whether S&T executes R&D projects in accordance with Federal and DHS guidelines, policies, and procedures.

We originally planned to focus our audit work on pilot projects. However, S&T was unable to provide the project status of all R&D projects at this level of detail. Therefore, we adjusted our audit objective and testing methodology to include all ongoing projects in the execution phase.

To accomplish our objective, we obtained and reviewed relevant Federal laws and OMB requirements. We also obtained and reviewed DHS and S&T policies, procedures, and guidance relating to R&D activities. We reviewed and analyzed prior OIG and GAO audit reports related to the audit objective.

We interviewed S&T officials from the four primary S&T offices: MCS, OIC, OSE, OES. We also interviewed officials in S&T's Office of Strategy and Policy and Privacy Office to obtain an understanding of S&T's organizational structure as well as their roles and responsibilities relating to R&D and their processes and procedures. Additionally, we met with the Chief of Staff Office, and Contract Acquisition Program Support, Finance and Budget, and the Program Support Office within OES to obtain a universe of R&D projects for our testing sample. Further, we met with the DHS Program Accountability Risk Management and Office of Management and Budget to obtain an understanding of project manager certification requirements. We also met with Office of Procurement Operations to obtain an understanding of the awarded contracts within our sample.

The Finance and Budget Division provided us a list of R&D projects managed by S&T that were in the execution phase during FY 2020. The list contained a total of 383 projects with obligations of approximately $309 million. During data validation, we discovered 14 of the 383 projects were in-house projects managed by OES. The team removed these 14 OES projects from our potential sampling universe, resulting in 369 projects with obligations totaling approximately $305 million.

To ensure coverage of projects executed by MCS, OIC, and OSE, we sorted the data provided by office. We then judgmentally selected a total of 24 projects to review. The following table provides the total number of projects and dollar

amount of obligations for each office and the number and dollar amount of projects selected for testing.

Universe of R&D Projects by S&T Office and Number Selected for Testing from Each Office

Office	Universe of Projects	Total Obligations	Number of Projects Selected	Percent of Selected Projects*	Obligations for Selected Projects	Percent of Selected Obligations*
MCS	230	$214,538,192	15	7%	$17,860,122	8%
OIC	77	$55,385,760	5	6%	$1,809,724	3%
OSE	62	$34,992,878	4	6%	$1,634,180	5%
Total	369	$304,916,830	24	7%	$21,304,026	7%

* Percent rounded to nearest whole number
Source: DHS OIG-prepared based on information in the list of R&D projects provided by S&T

We interviewed S&T officials to confirm the information for each project selected. However, the data field for the assigned project managers was inaccurate. As a result, S&T manually created an updated list of project managers that we used to obtain the project file for each of the 24 selected projects. We determined the project list to be sufficiently reliable for our audit purposes.

During our survey work we identified the checklist requirements and used them as a basis for developing our compliance tests. We also identified project management requirements from our review of the process flow. We then created a data collection instrument to test the 24 selected projects to determine whether S&T executed R&D projects in accordance with Federal and DHS guidelines, policies, and procedures.

We requested the entire project file from the assigned project manager for each selected project and reviewed information in the file to complete the data collection instrument. In some instances, the project files did not contain the documents we needed to perform our compliance tests. We followed up with the project managers as applicable to obtain the missing documents. We also requested project file documentation from Office of Procurement Operations for projects that were deemed high risk.

Other than obtaining and reviewing project documentation for each of the 24 selected projects, we did not perform data reliability testing for the remaining 345 projects in our universe of R&D projects, and we did not assess the completeness or accuracy of R&D projects. The scope of this audit was limited to assessing S&T's compliance with guidelines, policies, and procedures.

We identified control weaknesses in the control environment and monitoring internal control components. We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. We identified control weaknesses, as described in the Results of Audit section of this report. However, because we limited our review to the control environment and monitoring components, other internal control deficiencies may have existed at the time of our audit.

We conducted this audit between October 2020 and September 2021 pursuant to the *Inspector General Act of 1978, as amended*, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
S&T Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

February 17, 2022

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

GLENN S PODONSKY Digitally signed by GLENN S PODONSKY Date: 2022.02.17 10:59:15 -05'00'

FROM: Glenn Podonsky
Senior Component Accountable Official
Executive Director, Office of Enterprise Services
Science and Technology Directorate

SUBJECT: Management Response to Draft Report: "S&T Needs to Improve Its Management and Oversight of R&D Projects" (Project No. 20-039-AUD-S&T)

Thank you for the opportunity to comment on this draft report. The Science and Technology Directorate (S&T) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

Senior S&T leadership is pleased to note OIG's recognition that S&T works with Components in the U.S. Department of Homeland Security (DHS) to identify capability gaps in DHS operations, and to research and develop technologies to address those gaps. For example, during the last 3 years S&T implemented management systems to strengthen its project and financial management processes, including the:

1) Business Process Flow (BPF), which encompasses the entire process of gap identification, decomposition, project development, funding, execution, and transition; and

2) Science and Technology Analytical Tracking System (STATS), which is currently in use as the authoritative data source for all research and development projects.

S&T remains committed to enabling effective, efficient, and secure operations across all homeland security missions by applying scientific, engineering, analytic, and innovative approaches to deliver timely solutions and support departmental acquisitions.

The draft report contained 5 recommendations with which S&T concurs. Attached find our detailed response to each recommendation. S&T previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment

Attachment: Management Response to Recommendations Contained in 20-039-AUD-S&T

OIG recommended that the Senior Official Performing the Duties of the Under Secretary for S&T:

Recommendation 1: In consultation with the Office of Procurement Operations, develop and implement a process, to ensure required special clauses are included in contracts for project acquisitions with a high risk of unauthorized access to or disclosure of sensitive information.

Response: Concur. The S&T Compliance Division and the S&T Office of Contracts, Acquisition, and Program Support are collaboratively drafting a formal process, and associated implementation training, in consultation with the Office of Procurement Operations, to ensure the proper clauses are included in contracts for project acquisitions with a high risk of unauthorized access to, or disclosure of, sensitive information. Once complete, this formal process and training will be provided to Program Managers (PMs), Contract Officer Representatives, and staff in the S&T Compliance Division.

Additionally, in July 2021, a "Project Situational Compliance" Checklist was added as Appendix A to the current S&T internal Program and Project Management Plan templates, which requires PMs to consider all compliance requirements impacting their program prior to the Procurement Request submission. Estimated Completion Date (ECD): January 31, 2023.

Recommendation 2: Develop and implement a process, with a timeline, to ensure that project managers prepare Privacy Threshold Analyses for all projects and provide the analyses to the S&T Privacy Office for review.

Response: Concur. The S&T Compliance Director, in coordination with leadership across the Directorate and the S&T Program Support Office (PSO), is developing a process with associated timeline, checklists, and guidance to ensure that the privacy documentation, including the projected timeline with milestones, is developed, as appropriate. Once complete, this process will be formally communicated to program and project managers to ensure the requirements are understood. ECD: January 31, 2023.

Recommendation 3: Clarify the requirements for the preparation of Checklists for Sensitive Information, Privacy Threshold Analyses, project plans, update S&T guidance, and formally communicate the requirements to program and project managers.

Response: Concur. The process currently under development by the S&T Compliance Director, in coordination with leadership across the Directorate and the S&T PSO, to

3

ensure the development of the privacy documentation, including the projected timeline with milestones, as appropriate, will also address this recommendation. Once complete, this process will be formally communicated to program and project managers to ensure the requirements are understood. ECD: January 31, 2023.

Recommendation 4: Develop and implement a policy to require and track FAC-P/PM [Federal Acquisition Certification for Program and Project Managers] certification for research and development program and project managers that meets Office of Management and Budget [OMB] and Department of Homeland Security requirements.

Response: Concur. On December 1, 2021, the Director of Mission Capability Support issued a memorandum, "Federal Acquisition Certification for the Office of Mission and Capability Support (MCS) Program Managers (FAC-P/PM) Certification," requiring project management certifications for all program managers. PSO is coordinating with the Human Capital Office and S&T Principal Directors to enhance existing processes to also track PM certifications.

Additionally, OMB is currently rolling out the Competency Exploration for Development And Readiness tool, in coordination with the DHS Office of the Chief Human Capital Officer (OCHCO), during 2022. PSO is working with OCHCO and the Principal Directors to begin using this tool within S&T, which will collect data to baseline project management capabilities within the organization and identify areas where S&T needs to increase certifications and skills to appropriate levels. ECD: March 31, 2023.

Recommendation 5: Require that program and project managers use the Science and Technology Analytical Tracking System [STATS], or other centralized project management system, to track and manage all research and development projects.

Response: Concur. STATS is the current authoritative data source for all research and development projects. The Deputy Under Secretary for S&T will issue a formal memorandum requiring the use of STATS for all research and development projects. ECD: March 31, 2022.

4

Appendix C
Office of Audits Major Contributors to This Report

Richard Harsche, Audit Director
Peter Christopher, Audit Manager
Rolando Chavez, Auditor-in-Charge
Vera Cropp, Program Analyst
Juan Santana, Auditor
Thomas Hamlin, Communications Analyst
Peter Charboneau, Independent Reference Reviewer

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
S&T Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305