U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-47

August 20, 2024

FINAL REPORT

S&T Inconsistently Managed Critical Infrastructure Security and Resilience Research and Development Activities

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

August 20, 2024

MEMORANDUM FOR: The Honorable Dimitri Kusnezov, Ph.D.
Under Secretary
Science and Technology Directorate

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.08.19 16:23:36 -04'00'

SUBJECT: *S&T Inconsistently Managed Critical Infrastructure Security and Resilience Research and Development Activities*

Attached for your action is our final report, *S&T Inconsistently Managed Critical Infrastructure Security and Resilience Research and Development Activities*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving S&T's critical infrastructure research, development, testing, and evaluation efforts. Your office concurred with all four recommendations. Based on information provided in your response to the draft report, we consider recommendations 1, 3, and 4 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. Recommendation 2 is closed and resolved.

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 contact me with any questions, or your staff may Kristen Bernard, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

S&T Inconsistently Managed Critical Infrastructure Security and Resilience Research and Development Activities

August 20, 2024

Why We Did This Audit

S&T is responsible for leading the Department's research and development efforts. In 2021, S&T received $157.5 million in funding through the *Infrastructure Investment and Jobs Act* to address critical infrastructure R&D needs.

We conducted this audit to determine how well S&T has managed R&D activities aimed at improving critical infrastructure security and resilience.

What We Recommend

We made four recommendations to improve S&T's critical infrastructure R&D efforts.

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 Science and Technology Directorate (S&T) can improve management of its research, development, testing, and evaluation (R&D) activities related to critical infrastructure security and resilience. Although S&T is actively making efforts to improve processes, it:

- does not use a risk-based, holistic approach to prioritize critical infrastructure R&D programs and projects department-wide;
- does not follow established project management principles and its own project management policies and procedures; and
- relies on inaccurate and incomplete information to manage its critical infrastructure R&D projects.

These problems occurred because S&T relies on component-based R&D prioritization processes instead of establishing and updating department-wide strategic priorities. Additionally, S&T does not ensure adherence to project management best practices, such as integrating program and project plans, using standard terminology and abbreviations, and tailoring its processes to fit the project needs. Finally, S&T has no formal data validation process to ensure the quality of R&D project management data.

Without adequate controls in place to consistently plan, manage, and execute its R&D activities, S&T may not be able to support the Department's critical infrastructure R&D needs. The issues we identified also raise concerns as to S&T's ability to successfully plan, manage, and spend the $157.5 million in *Infrastructure Investment and Jobs Act* funding.

S&T Response

S&T officials concurred with all four recommendations and described corrective actions to address the issues we identified.

Table of Contents

Abbreviations

BPF	Business Process Flow
CISA	Cybersecurity and Infrastructure Security Agency
CISRR	Critical Infrastructure Security and Resilience Research Program
FFMS	Federal Financial Management System
GAO	U.S. Government Accountability Office
IIJA	*Infrastructure Investment and Jobs Act*
IPT	integrated product team
IRDC	Innovation, Research, and Development Coordination
MCS	Office of Mission Capability and Support
PEC	Program Element Code

PPD-21	Presidential Policy Directive 21
R&D	research, development, testing, and evaluation
S&T	Science and Technology Directorate
STATS	S&T Analytical Tracking System

Background

The Science and Technology Directorate (S&T) is the primary research and development arm of the Department of Homeland Security. The *Homeland Security Act of 2002*[1] gives the Secretary of DHS, acting through the Under Secretary for S&T, responsibility for establishing and administering the Department's research, development, testing, and evaluation (R&D) activities, including determining the long-term R&D needs and capabilities for all DHS components and coordinating and integrating all the Department's R&D activities. S&T is also responsible for leading R&D efforts to strengthen the security and resilience of the Nation's 16 critical infrastructure sectors.[2]

Two of S&T's four main offices have primary responsibility for conducting, managing, and overseeing critical infrastructure R&D activities:

- The Office of Mission Capability and Support (MCS) provides support through customer-focused implementation of programs based on validated priorities, gaps, and requirements. The office's main function is program management. MCS has five active programs related to critical infrastructure. See Appendix C for a list of MCS' critical infrastructure projects and programs.

- The Office of Innovation and Collaboration (Innovation and Collaboration) provides research, development, innovation, business capabilities, and expert solutions that address and help overcome operational challenges. Within this office, the Office of University Programs works with universities to establish S&T Centers of Excellence. Through these centers, S&T uses academia and private sector expertise to research and develop potential solutions for DHS operational challenges. Innovation and Collaboration has four Centers of Excellence related to critical infrastructure. See Appendix C for a list of Innovation and Collaboration's Centers of Excellence related to critical infrastructure.

The S&T Operating Model Blueprint (Blueprint),[3] in conjunction with the Business Process Flow (BPF),[4] serves as S&T's project management framework and details the processes for R&D efforts. Collectively, these documents standardize the R&D process, ensure engagement with S&T's

[1] Title 6 of the United States Code, Section 182.
[2] The Nation has 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The Cybersecurity and Infrastructure Security Agency (CISA) helps S&T safeguard critical infrastructure by enhancing stakeholder capacity to mitigate risks.
[3] Included within *Understanding S&T's Business Process Flow*, June 2022.
[4] The BPF expands the Blueprint into nine processes and seven decision points to ensure effective oversight and informed decision making through the life cycle of programs and projects.

customers, and enable effective oversight and informed decision making throughout the program and project life cycle. S&T acknowledged challenges with the BPF and contracted with the Homeland Security Operational Analysis Center (Analysis Center),[5] which is currently operated by the RAND Corporation,[6] to help identify areas of improvement. The Analysis Center issued its assessment in May of 2023 with various recommendations to improve the BPF process.

S&T tracks activities, including R&D, through its S&T Analytical Tracking System (STATS). This system contains acquisition, financial, and project management documentation that helps S&T track, manage, and administer effective program and project operations. Within STATS, S&T uses Program Element Codes (PEC) to track its program, project, and activity information. S&T also uses PECs in its financial system of record, the Federal Financial Management System (FFMS).[7]

Infrastructure Investment and Jobs Act

In November 2021, the President signed the *Infrastructure Investment and Jobs Act* (IIJA).[8] The IIJA provided S&T with $157.5 million (available through 2026) for critical infrastructure R&D projects in five focus areas, which are further described in Appendix D.

- Focus Area 1 - Special Event Assessment Rating Planning Tools[9]
- Focus Area 2 - Electromagnetic Pulse[10] and Geomagnetic Disturbance[11] Resilience Capabilities
- Focus Area 3 - Position, Navigation, and Timing Capabilities
- Focus Area 4 - Public Safety and Violence Prevention/Soft Target[12] Security
- Focus Area 5 - Security Testing Capabilities for Telecommunications Equipment, Industrial Control Systems, and Open-Source Software

To better manage and ensure proper execution of activities occurring within IIJA focus areas,

[5] S&T requested that the Analysis Center conduct an independent analysis of its BPF. In its May 2023 report to S&T, the Analysis Center described challenges related to governance and process ownership, gap intake and triage, collaboration, and centralized tracking of research and development activities. This review resulted in several recommendations that S&T is currently working on to improve its processes.
[6] The RAND Corporation is an independent nonprofit institution that helps develop solutions to public policy and decision-making challenges through its written publications.
[7] FFMS is owned and operated by U.S. Immigration and Customs Enforcement.
[8] P.L. 117-58, Division J.
[9] Special Event Assessment Ratings are applied to events that are not designated as a national special event. Most of these events are state and local events that may require additional support from the Federal Government.
[10] An electromagnetic pulse is a burst of electromagnetic energy produced by a nuclear explosion in the atmosphere, considered capable of widespread damage to power lines, telecommunications, and electronic equipment.
[11] A geomagnetic temporary disturbance of the Earth's magnetosphere caused by a solar wind shock wave and/or cloud of magnetic field that interacts with the Earth's magnetic field.
[12] A soft target is a target that can be attacked easily because it does not have military defenses.

S&T created the Critical Infrastructure Security and Resilience Research (CISRR) Program. MCS is responsible for implementing the program.

We conducted this audit to determine how well S&T has managed R&D activities aimed at improving critical infrastructure security and resilience for fiscal years 2018 through 2022. Our audit focused on Focus Areas 2 (Electromagnetic Pulse and Geomagnetic Disturbance Resilience Capabilities) and 4 (Public Safety and Violence Prevention/Soft Target Security). These two focus areas had a combined budget of $71,800,000 in IIJA funding ($22,750,000 for Focus Area 2 and $49,050,000 for Focus Area 4).

Results of Audit

S&T can improve management of its R&D activities related to critical infrastructure security and resilience. Although S&T is actively making efforts to improve processes, it:

- does not use a risk-based, holistic approach to prioritize critical infrastructure R&D programs and projects department-wide;
- does not follow established project management principles and its own project management policies and procedures; and
- relies on inaccurate and incomplete information to manage its critical infrastructure R&D projects.

These problems occurred because S&T relies on component-based R&D prioritization processes instead of establishing and updating department-wide strategic priorities. Additionally, S&T does not ensure adherence to project management best practices, such as integrating program and project plans, using standard terminology and abbreviations, and tailoring its processes to fit the project needs. Finally, S&T has no formal data validation process to ensure the quality of R&D project management data.

Without adequate controls in place to consistently plan, manage, and execute its R&D activities, S&T may not be able to support the Department's critical infrastructure R&D needs. The issues we identified also raise concerns as to S&T's ability to successfully plan, manage, and spend the $157.5 million in IIJA funding.

S&T Did Not Use a Risk-Based, Holistic Approach to Prioritize Its Critical Infrastructure R&D Programs and Projects Department-Wide

The *Homeland Security Act of 2002* tasks S&T with establishing and administering R&D activities for the Department, including long-term research and development needs and capabilities for all elements of the Department. Presidential Policy Directive 21, *Critical Infrastructure Security and*

Resilience (PPD-21)[13] recommends that the DHS Secretary, who subsequently delegated responsibility to S&T,[14] issue and update a National Critical Infrastructure Security and Resilience Research and Development Plan every 4 years (or more frequently, if necessary). The plan should identify priorities and guide R&D requirements and investments. The plan should also set priorities for the entire critical infrastructure community beyond DHS, including Federal, state, and local government and the private sector. Finally, S&T's 2021 strategic plan[15] calls for an annual threat assessment report to help inform R&D investments.

S&T did not use a formal risk-based process to prioritize R&D needs on a department-wide basis. Instead of prioritizing R&D needs using the strategic-level plans, such as the National Critical Infrastructure Security and Resilience Research and Development Plan and annual strategic plans, S&T relied on DHS components to establish the prioritization of R&D needs. According to S&T officials, S&T subject matter experts work with components to prioritize their identified R&D needs. However, an S&T official stated these needs are very compartmentalized. S&T will then execute components' identified R&D efforts once funding becomes available. All the activities funded by the IIJA were R&D needs previously identified by components.

This occurred because S&T changed its process for identifying and prioritizing R&D projects to be based on customer-focused (as opposed to mission-focused) R&D needs and did not complete R&D strategic planning documents and its strategic plan. In 2018, S&T implemented a customer needs-driven, integrated product team (IPT)[16] approach to its work at the component level. According to the Analysis Center's assessment of S&T's processes, each component has a different level of maturity and capability. According to an S&T official, some components do not have an IPT and, as a result, the applicability and quality of components' gaps varied greatly. This means the Department does not have a standardized IPT process for identifying risks and prioritizing R&D projects across DHS components. Although an S&T official stated they try to prioritize R&D gaps identified by multiple components, there is no process to perform cross-portfolio analysis to weigh, rank, or score projects to determine which projects to fund. The S&T official also stated that S&T attempts to fund at least one of each component's top priorities regardless of relative risk or value.

DHS and S&T have published 2023 strategic priorities[17] that provide guidance to components for assessing capability gaps. Even so, S&T has not published threat assessment and strategic policy documents that could aid in identifying and prioritizing R&D activities for itself, the Department,

[13] On April 30, 2024, the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22) was published. This memorandum rescinded and replaced PPD-21.
[14] PPD-21 tasks the DHS Secretary with this responsibility. DHS Delegation Number 10001 Rev. 01 (April 28, 2014) delegates all PPD-21 R&D responsibilities to the Under Secretary of S&T.
[15] *S&T Strategic Plan 2021*.
[16] IPTs consist of S&T and component officials. These teams address specific issues relevant to the mission and align R&D investments with operational gaps and planned acquisitions.
[17] DHS 2023 Priorities and S&T's Calendar Year 2023 Priority Areas.

and all its critical infrastructure partners. Specifically, it has not updated the National Critical Infrastructure Security Resilience Research and Development Plan recommended by PPD-21 since its issuance in 2015. Given that PPD-21 recommends the National Critical Infrastructure Security Resilience Research and Development Plan be updated every 4 years, S&T should have published updated versions in 2019 and 2023 but did not. Moreover, during our audit, S&T was unable to provide us with information on who in the organization was responsible for updating the plan.

S&T has yet to publish an annual threat assessment report, as called for by its own 2021 Strategic Plan. According to an S&T official, threat assessments are no longer required because of other annual priority publications such as the DHS 2023 Priorities and S&T's Calendar Year Priority Areas. S&T also noted that in January of 2023, DHS established the Innovation, Research, and Development Coordination (IRDC) Council to address the need to prioritize R&D efforts. The IRDC is co-chaired by the Undersecretary for S&T and serves as the executive governing body for the DHS R&D coordination process.[18] The goal of the IRDC is to help the Department identify strategic priority research issues.

Instead of updating these strategic documents and establishing a risk-based process for selecting R&D projects, S&T decided to spend the $157.5 million in IIJA funds for R&D activities without evaluating the projects' strategic value across DHS. Further, because S&T has not updated the National Critical Infrastructure Security and Resilience Research and Development Plan, other critical infrastructure partners may be unaware of priority critical infrastructure needs and apply their efforts to less strategic and advantageous programs and projects. Given these factors, S&T may not be using IIJA and other R&D funds to address the Nation's highest risks. In May 2024, after the end of our audit scope, DHS published the *DHS Innovation, Research & Development Strategic Plan,* which includes information collected in FY 2023, such as innovation, research, and development of current state initiatives; emerging technologies analyses; and individual operational component future trends assessments. The plan also assesses trends across future capabilities and points to opportunities for the Department to use innovation, research, and development in a cross-cutting manner to advance DHS' missions and objectives.

[18] The IRDC was established after the end of our audit scope. As such, we did not test the implementation of the IRDC or how it impacts S&T's critical infrastructure R&D efforts.

S&T Did Not Follow Established Project Management Principles, Policies, and Procedures

The Project Management Institute[19] established standards on effective project and program management practices, and S&T has its own established policies and procedures. However, S&T did not adhere to the recommended standards or its own policies and procedures.

The Project Management Institute's *A Guide to the Project Management Body of Knowledge* [20] and *The Standard for Program Management* [21] include leading practices for program and project management that can be applied to S&T R&D activities. Specifically:

- It is the program manager's responsibility to ensure alignment of individual project management plans with the program's goals.
- The program management plan should integrate the program's subsidiary project plans. This ensures the projects and programs are aligned with the strategic priorities of the organization to deliver expected benefits.
- Project teams should tailor the project management framework to enable the flexibility to consistently produce positive outcomes within the context of the project life cycle. This includes taking specific action to select and mix specific project elements to suit the unique characteristics of the project and project environment.

S&T's Blueprint[22] outlines high-level foundational processes that enable common program and project management practices for R&D efforts, including establishing a project management framework and processes for all discretionary research, development, and innovation-funded capability gap initiatives. S&T's BPF[23] further outlines processes and decision points for assessing outcomes to ensure compliance with the Blueprint for projects and programs. Appendix E shows S&T's BPF processes and decision points. The BPF is designed to be tailored to meet the needs of individual projects, allowing for the BPF to be adjusted to meet the needs of the specific gap or need.

These processes include developing project plans containing work breakdown structures, milestones/schedules, budget, communication plans, test and assessment plans, and a

[19] According to *Program Management: DOE Needs to Develop a Comprehensive Policy and Training Program,* GAO-17-51, November 2016, the Project Management Institute has established a standard on program management that is generally recognized as a leading practice for most programs.
[20] Project Management Institute's *A Guide to the Project Management Body of Knowledge*, 6th Edition.
[21] Project Management Institute's *The Standard for Program Management*, 4th Edition.
[22] Included within *Understanding S&T's Business Process Flow*, June 2022.
[23] *Understanding S&T's Business Process Flow*, June 2022.

transition strategy. The BPF also requires managers to integrate the project plan into a program management plan if the project is part of a larger program.

We found that S&T did not consistently manage critical infrastructure R&D programs and projects per the Project Management Institute standards, Blueprint, or BPF processes. Specifically:

- <u>MCS</u> — We determined MCS did not always develop program and project management plans for its R&D activities. Specifically:
    - One of the six MCS programs[24] reviewed did not have a program management plan.
    - Seven of nine MCS critical infrastructure projects reviewed did not have project management plans. Instead, project managers used program management plans to govern project execution. However, program management plans do not contain the level of detail, such as milestones, staffing plans, and deliverables, needed to adequately execute, monitor, and control projects.
- <u>Innovation and Collaboration</u> — Even though S&T designed the framework to be tailored to meet the needs of individual projects, Innovation and Collaboration neither follows the BPF process nor has any other policies in place of the BPF to ensure it adheres to the Blueprint. As a result, S&T uses inconsistent definitions of program and project, which further prevents S&T management from providing effective oversight of its critical infrastructure R&D efforts. Innovation and Collaboration uses program management plans for each Center of Excellence, and in turn, uses work plans written by the centers to govern individual efforts. Innovation and Collaboration considers each Center of Excellence as a "program." However, STATS denotes "DHS Centers" as a program and the individual centers as projects.

These issues occurred because S&T does not have consistent policies and procedures to ensure its offices responsible for critical infrastructure R&D adhere to program and project management best practices, such as integrating program and project plans, using standard terminology and abbreviations, and tailoring their processes to fit the project needs. For example, S&T's BPF implementation templates use "PMP" interchangeably for "program management plan" and "project management plan." Similarly, the BPF uses "PM" as an abbreviation for both "project manager" and "program manager," leaving ambiguity regarding who is responsible for managing different pieces of the process, including integrating the project plan into the program plan.

[24] The Explosives Detection program was discontinued and transitioned to Physical Security.

What we found is consistent with a previous DHS Office of Inspector General report[25] and the Analysis Center's assessment of S&T's processes. We reported in 2022 on privacy and contracting issues within S&T and identified concerns regarding the lack of project plans. In 2023, the Analysis Center identified an issue with the lack of a single BPF process owner to provide overall governance and management resulting in patchwork accountability, siloed management, poorly documented sub-processes, duplication of efforts, and delays in meeting component needs.

S&T officials stated resource constraints and mission differences between MCS and Innovation and Collaboration impact the offices' abilities to consistently follow the Blueprint or other best practices. For example, MCS has used either the program or project plan interchangeably and does not ensure integration of project management plans into the higher-level program management plan because it does not have the resources to create and integrate both documents. This limits management's ability to monitor and control projects or measure execution against cost and schedule baselines. The two offices also have different requirements for customer agreement. MCS does not begin developing a project until the customer agrees it is a viable solution. Conversely, Innovation and Collaboration takes a broader perspective, with the Office of University Programs providing management and oversight of the Centers of Excellence's activities. However, the Centers of Excellence establish their own annual workplans. Without applying its own framework and processes, as well as program and project management best practices, S&T cannot ensure effective oversight and informed decision making for its critical infrastructure R&D efforts, including those funded by the IIJA.

S&T Relies on Incomplete and Inaccurate Information to Manage Its Critical Infrastructure R&D Projects

According to the U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*,[26] management should have relevant data from reliable sources and data processed into quality information to inform decisions. In response to a recommendation from our prior audit of S&T,[27] the Senior Official Performing the Duties of the Under Secretary for S&T issued a June 8, 2022, memorandum mandating that all staff use STATS to track and manage all R&D projects across the Directorate. The memorandum requires that STATS contain all project-related information, including authoritative, organization, and contact data, and quarterly updates to key milestones and transitions. The memorandum also notes that STATS should serve as an interconnected database of financial and budget tools to support data analysis and reporting across S&T. Through STATS, S&T can ensure the successful collection and appropriate reporting of key information required to inform decision making.

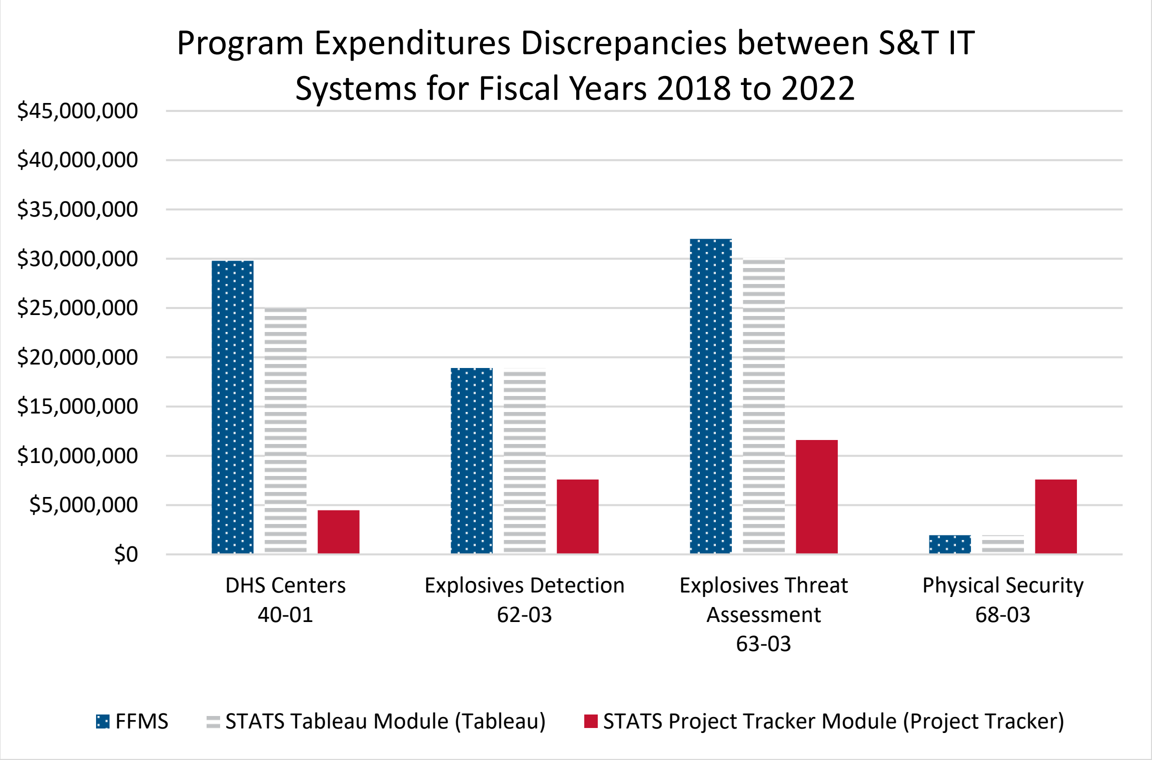
[25] *S&T Needs to Improve Its Management and Oversight of R&D Projects,* OIG-22-30, March 7, 2022.
[26] *Standards for Internal Control in the Federal Government*, GAO-14-704G, September 2014.
[27] *S&T Needs to Improve Its Management and Oversight of R&D Projects,* OIG-22-30, March 2022.

S&T project managers do not consistently use STATS to track project performance, as required, and do not ensure STATS records are up to date. We determined STATS included incomplete or inaccurate project information. For example, we reviewed records for 14 critical infrastructure-related projects and determined that 9 of 14 (64 percent) projects had inconsistent and incomplete information:

- four projects did not include active or met milestones;
- one project was missing from the system; and
- four projects contained inconsistent titles.

We also identified STATS modules containing inconsistent and incomplete financial information for four of the seven (57 percent) programs reviewed, as depicted in Figure 1. Additionally, information in STATS did not match information in FFMS.

Figure 1. Discrepancies in Financial Data between S&T's IT Systems



Source: DHS OIG analysis of FFMS and STATS data

These issues align with the Analysis Center's independent review identifying challenges with data and information management. Specifically, the Analysis Center concluded S&T does not have data governance and highlighted the need for enterprise-level oversight and authority. The Analysis Center noted S&T has multiple systems that do not communicate with each other, and this has led to delays in S&T's ability to integrate the data between the systems.

S&T does not ensure compliance with internal control standards and best practices or with its own internal requirement to use STATS for a number of reasons. For example:

- At least two project managers track project information on a SharePoint site and rely on institutional knowledge of the project's history to manage their projects.
- S&T's offices do not have a consistent definition or application for the terms "program," "project," and "activity," resulting in inconsistent levels of program and project information necessary for decision makers to compare and monitor efforts.
- S&T predominately uses a manual process to transfer data from FFMS into STATS, resulting in numerous errors. Transfer errors contributed to inaccurate information in STATS that financial and budget personnel did not reconcile during our audit.
- S&T does not have a standardized data validation process for reconciling data inaccuracies between STATS and FFMS. According to S&T personnel, they usually identify about 200 discrepancies out of 8,000- or 9,000- line items during their manual review that need correction.

As a result, S&T relies on incomplete and inaccurate data to track and manage its projects and programs and make decisions about program operations and continued funding. This issue will be exacerbated if staff and subject matter experts leave, taking institutional knowledge with them.

Conclusion

S&T's strategic documents have a far-reaching impact across all 16 critical infrastructure sectors. Instead of updating strategic plans to inform a risk-based approach, S&T focuses on individual customer R&D requests. By doing so, S&T cannot ensure that the Department's highest priority critical infrastructure R&D needs are addressed. Without improved project and data management practices, S&T also cannot ensure effective use of current project funding, including the $157.5 million of IIJA funding available to address critical infrastructure R&D needs.

Recommendations

Recommendation 1: We recommend the Under Secretary for S&T clearly identify the appropriate entity with the authority and responsibility for updating critical infrastructure research and development strategic plans and annual homeland threat assessments and ensure that entity publishes each document in accordance with each of the prescribed timeframes.

Recommendation 2: We recommend the Under Secretary for S&T establish a formal, risk-based process that incorporates strategic plans and threat assessments to prioritize the Department's research, development, testing, and evaluation projects and activities identified by the components and integrated product teams.

Recommendation 3: We recommend the Under Secretary for S&T develop and implement improved controls to ensure all S&T offices adhere to program and project management principles per the Operating Model Blueprint, including, but not limited to, policies, procedures, and training. These controls should ensure that tailored project approaches are documented and approved, standardized project management language is used, project and program plans are appropriately integrated, and roles and responsibilities are clearly defined.

Recommendation 4: We recommend the Under Secretary for S&T develop and implement data validation controls to ensure accurate and consistent financial and project information in S&T's centralized project tracking system, including, but not limited to, implementation policies, procedures, and training.

Management Comments and OIG Analysis

In response to our draft report, S&T officials concurred with all four recommendations and described corrective actions to address the issues we identified. We consider Recommendations 1, 3, and 4 open and resolved and Recommendation 2 closed and resolved. Appendix B contains S&T's management response in its entirety. We also received technical comments on the draft report and revised the report as appropriate. A summary of S&T's response and our analysis follows.

S&T Response to Recommendation 1: Concur. The S&T Office of Strategy and Policy is primarily responsible for coordinating and publishing applicable R&D plans, to include updating guidance that removes any S&T requirement to produce threat assessments under the exclusive purview of other DHS components and offices, as appropriate. Further, S&T will work closely with CISA in CISA's development of the National Infrastructure Risk Management Plan, which will be informed by sector-specific and cross-sector risk assessments. Following finalization of the National Infrastructure Risk Management Plan, S&T will produce an R&D plan to address critical infrastructure R&D needs. S&T will also continue to use its IPT with CISA and the *DHS Innovation, Research & Development Strategic Plan* to identify DHS-wide/cross-component critical infrastructure R&D priorities. The estimated completion date is August 29, 2025.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when S&T publishes and provides updated guidance and a critical infrastructure R&D plan.

S&T Response to Recommendation 2: Concur. To apply a risk-based approach to identify DHS-wide/cross-component R&D priorities, S&T uses the IRDC Council, which was chartered in

January 2023. The analysis performed under the IRDC Council enables S&T, and DHS as a whole, to optimize investment, reduce the risk of duplication, ensure complementary efforts, and focus on common challenges regarding DHS R&D projects and activities. Additionally, the *DHS Innovation, Research & Development Strategic Plan* integrates internal DHS strategies and provides external partners with Department gaps for future partnerships. This Plan addresses the objective to strengthen the security and resilience of critical infrastructure by identifying future innovation, research, and development capabilities needed for mission success through FY 2030.

OIG Analysis: S&T provided a copy of the May 2024 *DHS Innovation, Research & Development Strategic Plan* and the January 2023 *Innovation, Research, and Development Coordination Council Charter,* satisfying the intent of the recommendation. This, combined with the integration of these strategic documents into S&T's program management process as discussed in response to Recommendation 3, meets the intent of this recommendation. We consider this recommendation closed and resolved.

S&T Response to Recommendation 3: Concur. In addition to implementing recommended improvements identified in the Analysis Center report, S&T is now planning updates, as appropriate, to strengthen the current BPF with an updated BPF 3.0, which is being planned for completion before the end of FY 2024. S&T is also currently drafting updated IPT guidebooks, which will integrate BPF decision-making, provide direct tie-in to the *DHS Innovation, Research & Development Strategic Plan*, and provide more instruction on cross-component analysis. The estimated completion date is August 29, 2025.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when S&T provides documentation related to the BPF 3.0 update and any other program management policies and directives to cover all of S&T's critical infrastructure R&D activities across all divisions, relevant training material to educate staff, and updated IPT guidebooks.

S&T Response to Recommendation 4: Concur. S&T's Finance and Budget Division will conduct informational sessions/trainings to demonstrate how STATS can be used to track project information to ensure policies and procedures are being followed, as well as provide clear expectations of when to use the terms "program, "project," and "activity." In October 2023, S&T's Finance and Budget Division initiated corrective actions to identify and correct inaccuracies and inconsistencies between the FFMS and STATS data, and by January 2024 the division had established a data cleansing team and began developing several data visualization tools. The estimated completion date is August 29, 2025.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when S&T provides documentation such as updated policies and procedures mandating the use of STATS, training material, policies and procedures used by the cleansing team along with actions taken, and proof of implementation of STATS data visualization tools.

Appendix A:
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine how well S&T has managed R&D activities aimed at improving critical infrastructure security and resilience. The scope included two focus areas outlined in the IIJA: Focus Area 2 (Electromagnetic Pulse and Geomagnetic Disturbance Resilience Capabilities) and Focus Area 4, (Public Safety and Violence Prevention/Soft Target Security) and the related PECs for FYs 2018 through 2022.

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

We conducted interviews with S&T officials and obtained relevant documents from various offices to better understand roles and responsibilities related to critical infrastructure R&D activities, including policies and procedures followed and funding. These interviews included, but were not limited to:

- Office of Enterprise Services
- MCS
- Office of Science and Engineering
- Innovation and Collaboration
- Strategy and Policy Office
- Finance and Budget Division

We also interviewed data systems and financial management officials and the program and project managers responsible for the projects included in our review. Additionally, we obtained relevant documents related to the BPF and S&T's systems, including STATS and FFMS.

We determined S&T used 13,044 PECs during the audit period of FYs 2018 through 2022. From these, we identified and reviewed 23 PECs consisting of 14 critical infrastructure projects (9 MCS and 5 Innovation and Collaboration) and 7 programs (6 MCS and 1 Innovation and Collaboration).

We assessed internal controls related to S&T's management of R&D activities. We identified weaknesses with S&T's reliance on components' prioritization processes, not using project management best practices, and not validating R&D project management data. These internal control deficiencies are discussed in the “Results of Audit” section of this report. Because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

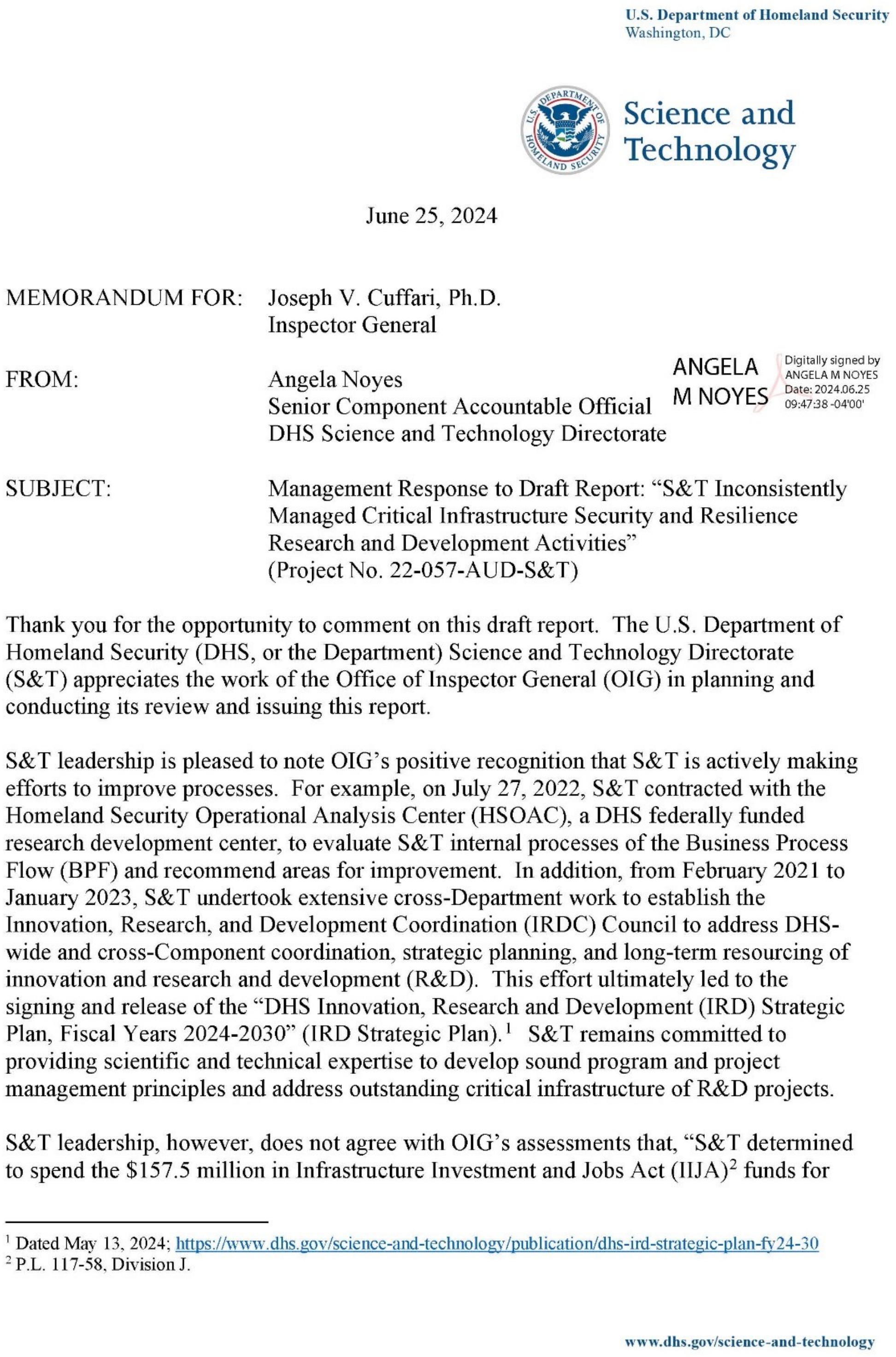
As part of this audit, we coordinated with the DHS OIG Office of Innovation’s Data Services Division, which provided technical support. To determine data reliability, the DHS OIG Office of Innovation’s Data Services Division obtained access to S&T information systems and coordinated with the audit team to provide various system reports for use in our review. Using information from these reports and S&T-provided data, we assessed and reconciled the completeness and accuracy of the PECs, obligations, and expenditures. We determined the PEC universe was sufficiently reliable, and we identified and reviewed 14 critical infrastructure projects. However, as documented in our report, we determined that expenditures and obligations were unreconcilable across S&T’s two systems, FFMS and STATS. Although information system control deficiencies were identified, as described in the body of the report, we determined the subsequent data in FFMS was sufficiently reliable for the purposes of this audit.

We conducted this audit from September 2022 through April 2024, pursuant to the *Inspector General Act of 1978*, 5 United States Code §§ 401–424, 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS OIG’s Access to DHS Information

During this audit, S&T provided timely responses to our requests for information and did not delay or deny access to information we requested.

Appendix B:
S&T Comments on the Draft Report



U.S. Department of Homeland Security
Washington, DC

Science and Technology

June 25, 2024

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

FROM: Angela Noyes
Senior Component Accountable Official
DHS Science and Technology Directorate

ANGELA M NOYES Digitally signed by ANGELA M NOYES Date: 2024.06.25 09:47:38 -04'00'

SUBJECT: Management Response to Draft Report: "S&T Inconsistently Managed Critical Infrastructure Security and Resilience Research and Development Activities"
(Project No. 22-057-AUD-S&T)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) 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.

S&T leadership is pleased to note OIG's positive recognition that S&T is actively making efforts to improve processes. For example, on July 27, 2022, S&T contracted with the Homeland Security Operational Analysis Center (HSOAC), a DHS federally funded research development center, to evaluate S&T internal processes of the Business Process Flow (BPF) and recommend areas for improvement. In addition, from February 2021 to January 2023, S&T undertook extensive cross-Department work to establish the Innovation, Research, and Development Coordination (IRDC) Council to address DHS-wide and cross-Component coordination, strategic planning, and long-term resourcing of innovation and research and development (R&D). This effort ultimately led to the signing and release of the "DHS Innovation, Research and Development (IRD) Strategic Plan, Fiscal Years 2024-2030" (IRD Strategic Plan).[1] S&T remains committed to providing scientific and technical expertise to develop sound program and project management principles and address outstanding critical infrastructure of R&D projects.

S&T leadership, however, does not agree with OIG's assessments that, "S&T determined to spend the $157.5 million in Infrastructure Investment and Jobs Act (IIJA)[2] funds for

[1] Dated May 13, 2024; https://www.dhs.gov/science-and-technology/publication/dhs-ird-strategic-plan-fy24-30
[2] P.L. 117-58, Division J.

www.dhs.gov/science-and-technology

R&D activities without evaluating the projects' strategic value across DHS" or that "S&T may not be using IIJA and other R&D funds to address the Nation's highest risks." In fact, throughout this audit, S&T provided OIG with documentation and comments demonstrating the mindful approach S&T took with IIJA funding. On April 25, 2022, for example, S&T created the Critical Infrastructure Security and Resilience Research (CISRR) program in response to the IIJA, working with the Cybersecurity and Infrastructure Security Agency (CISA), the Transportation Security Administration (TSA), and the DHS Special Events Program on the approach CISRR would take. As part of the Department's deliberate and thoughtful approach to evaluate the strategic value of these R&D activities, the CISRR effort to address the IIJA took into consideration Research, Development, Test and Evaluation (RDT&E) needs identified by CISA, TSA, and the Special Events Program, as well as information from CISA risk advisors regarding working with partners to defend against threats and collaborating to build a more secure and resilient infrastructure for the future.

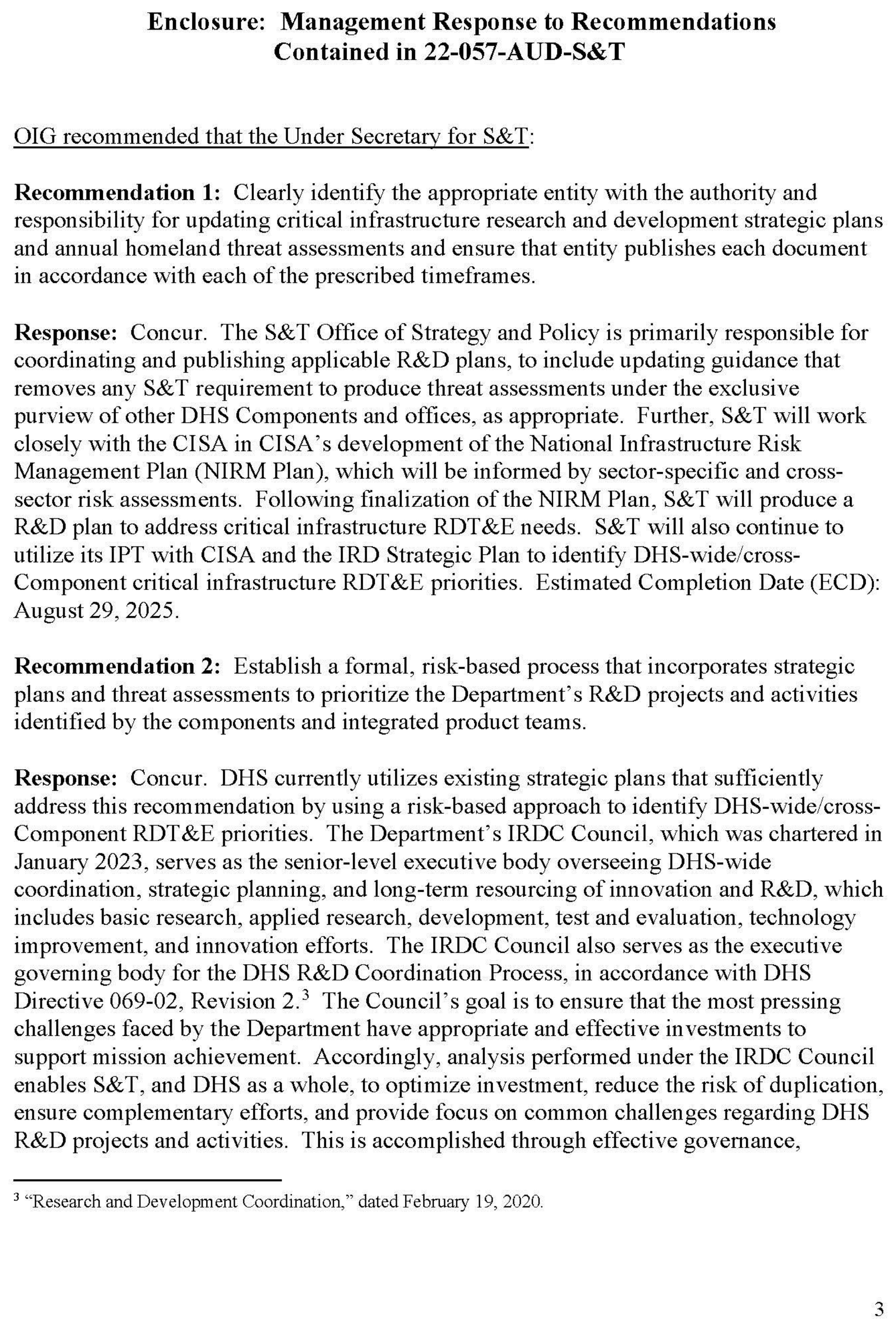
Further, the appropriate R&D focus areas for IIJA funds, as specified in the IIJA legislation, included areas of research for which S&T and CISA had previously unfunded requirements (i.e., projects) that had been through the review and selection process. To address risk in their R&D efforts, S&T utilizes twelve DHS Component Integrated Product Teams (IPTs), five Component collaborations (non-IPTs), and the IRDC Council to inform S&T investment strategies, each of which consider the risk landscape. It is inaccurate and misleading to suggest that these activities are not addressing risk, or collectively not addressing the Nation's highest risks.

It is also important to note that, over the years, S&T's budget has fluctuated from $1.4 billion in fiscal year (FY) 2006 to $744 million in FY 2024, making it difficult to execute planned R&D activities. The IIJA funding allowed S&T the opportunity to develop sound program and project management principles and address outstanding critical infrastructure projects not previously selected due to limited funding.

The draft report contained four recommendations with which S&T concurs. Enclosed find our detailed response to each recommendation. S&T previously submitted technical comments addressing several accuracy, context, 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.

Enclosure



Enclosure: Management Response to Recommendations Contained in 22-057-AUD-S&T

OIG recommended that the Under Secretary for S&T:

Recommendation 1: Clearly identify the appropriate entity with the authority and responsibility for updating critical infrastructure research and development strategic plans and annual homeland threat assessments and ensure that entity publishes each document in accordance with each of the prescribed timeframes.

Response: Concur. The S&T Office of Strategy and Policy is primarily responsible for coordinating and publishing applicable R&D plans, to include updating guidance that removes any S&T requirement to produce threat assessments under the exclusive purview of other DHS Components and offices, as appropriate. Further, S&T will work closely with the CISA in CISA's development of the National Infrastructure Risk Management Plan (NIRM Plan), which will be informed by sector-specific and cross-sector risk assessments. Following finalization of the NIRM Plan, S&T will produce a R&D plan to address critical infrastructure RDT&E needs. S&T will also continue to utilize its IPT with CISA and the IRD Strategic Plan to identify DHS-wide/cross-Component critical infrastructure RDT&E priorities. Estimated Completion Date (ECD): August 29, 2025.

Recommendation 2: Establish a formal, risk-based process that incorporates strategic plans and threat assessments to prioritize the Department's R&D projects and activities identified by the components and integrated product teams.

Response: Concur. DHS currently utilizes existing strategic plans that sufficiently address this recommendation by using a risk-based approach to identify DHS-wide/cross-Component RDT&E priorities. The Department's IRDC Council, which was chartered in January 2023, serves as the senior-level executive body overseeing DHS-wide coordination, strategic planning, and long-term resourcing of innovation and R&D, which includes basic research, applied research, development, test and evaluation, technology improvement, and innovation efforts. The IRDC Council also serves as the executive governing body for the DHS R&D Coordination Process, in accordance with DHS Directive 069-02, Revision 2.[3] The Council's goal is to ensure that the most pressing challenges faced by the Department have appropriate and effective investments to support mission achievement. Accordingly, analysis performed under the IRDC Council enables S&T, and DHS as a whole, to optimize investment, reduce the risk of duplication, ensure complementary efforts, and provide focus on common challenges regarding DHS R&D projects and activities. This is accomplished through effective governance,

[3] "Research and Development Coordination," dated February 19, 2020.

oversight, coordination, and guidance to all DHS and Component-level programs conducting innovation and R&D in support of DHS capabilities and mission objectives.

The Department's IRD Strategic Plan for FY 2024-2030 integrates internal DHS strategies and provides external partners with Department demand signals for future partnerships. From February to October 2023, S&T's Operations and Requirements Analysis (ORA) division worked with all DHS Components and offices to build this IRD Strategic Plan, to include inventorying current IRD activities; conducting a strength, weakness, opportunities, and threat analysis; holding a futures workshop; collecting Component future trend assessments (risks, threats, challenges); and reviewing national, DHS, and Component IRD strategies and guidance. S&T's ORA also held a public Technology and Innovation Network workshop on October 30, 2023, to present and gather feedback on the plan. In addition, the IRD Strategic Plan highlights complementary efforts underway across the DHS Homeland Security Enterprise (HSE), which consists of federal, state, local, tribal, territorial, nongovernmental, and private sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of the United States and its people.

Further, the IRD Strategic Plan inventories current and future IRD efforts within DHS, organized by the DHS Missions and Objectives in The Third Quadrennial Homeland Security Review.[4] By capturing these initiatives in a comprehensive plan, the Department can better align IRD to the desired outcomes of the DHS Missions and Objectives, as well as identify cross-cutting IRD themes that provide opportunities for making impacts towards meeting multiple desired outcomes. These initiatives are articulated as Strategic Priority Research Areas (SPRAs), which are cross-cutting assemblies of enduring scientific efforts that provide a means for addressing priority needs across multiple HSE mission areas and provide the Department an overarching path for future investments for FY 2024-2030. The identified SPRAs include: (1) Advanced Sensing; (2) Artificial Intelligence and Autonomous Systems; (3) Biotechnology; (4) Climate Change; (5) Communications and Networking; (6) Cybersecurity; (7) Data Integration, Analytics, Modeling, and Simulation; and (8) Digital Identity and Trust.

In addition, the IRD Strategic Plan addresses the objective to strengthen the security and resilience of critical infrastructure by identifying future IRD capabilities needed for mission success through FY 2030. Specifically, DHS must detect and prevent threats to critical infrastructure on which National Critical Functions (NCFs) rely, while also improving critical infrastructure's security, resilience, and attack mitigation. Doing so will minimize the impact of attempts to infiltrate, exploit, disrupt, or destroy critical infrastructure systems, networks, and NCFs they enable.

[4] Dated April 2023; https://www.dhs.gov/quadrennial-homeland-security-review.

However, DHS cannot mitigate threats it does not see, which requires expanding its operational visibility of threats to critical infrastructure. DHS S&T, to include ORA and several other offices coordinating as appropriate, is planning substantial future IRD to provide research and tools for event risk assessments; protection against impacts of climate change, electromagnetic pulses, and geomagnetic disturbance; protection of position, navigation, and timing systems; public safety for soft targets and crowded places; testing of new telecommunications equipment; exploration of artificial intelligence and machine learning to increase resiliency; testing and security of industrial control systems; and security for open-source software. The following SPRAs are expected to make impacts in meeting desired outcomes associated with this objective: Advanced Sensing; Artificial Intelligence and Autonomous Systems Biotechnology; Climate Change; and Cybersecurity.

S&T requests that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 3: Develop and implement improved controls to ensure all S&T offices adhere to program and project management principles in accordance with the Operating Model Blueprint, including, but not limited to, policies, procedures, and training. These controls should ensure that tailored project approaches are documented and approved, standardized project management language is used, project and program plans are appropriately integrated, and roles and responsibilities are clearly defined.

Response: Concur. S&T agrees with the importance of continuously tracking, evaluating, and improving internal processes to become more efficient and effective. In 2022, for example, senior S&T leadership recognized the need to improve internal processes of the BPF 2.0 version, and hired the HSOAC to perform an assessment and provide recommended areas of improvement to the effectiveness and efficiency of BPF 2.0. On November 15 and 16, 2022, S&T ORA conducted Directorate wide workshops in coordination with HSOAC to gain current perspectives as a baseline, and on February 28, 2023, a second Directorate wide workshop was conducted in coordination with HSOAC to review potential recommended improvements. HSOAC completed their assessment and provided recommendations in May 2023. S&T has since addressed these HSOAC recommendations, and in June 2023, S&T leadership took actions to address these recommendations, and issued decisions to improve the following four critical areas of the BPF:

(1) Governance and Process Ownership;
(2) BPF Process Management Office;
(3) Intake and Triage and R&D Lifecycle Teams; and
(4) Centralized Tracking of R&D efforts.

Since implementation of these decisions, S&T has seen tremendous improvement, such as (but not limited to) a reduction in time between intake and project/activity approval from 15 months to 6 months (conduct prioritization, decomposition, tech scouting, solution analysis, business case analysis, project pitch, and approval), which amounts to a 250 percent increase in efficiency. This improvement also includes the creation of a centralized BPF tracker system that monitors and reports RDT&E needs as they progress through the lifecycle, integration of internal matrix teams and standards, tailoring of approaches to identified RDT&E needs, and creation of a change control board configuration. Currently, S&T is now pursuing updates, as appropriate, to strengthen BPF 3.0, which is being planned for completion before the end of FY 2024. S&T is also currently drafting updated IPT Guidebooks, which will include integration of BPF decision-making, provide direct tie-in to the IRD Strategic Plan, and provide more instruction on cross-component analysis. ECD: August 29, 2025.

Recommendation 4: Develop and implement data validation controls to ensure accurate and consistent financial and project information in S&T's centralized project tracking system, including, but not limited to, implementation policies, procedures, and training.

Response: Concur. S&T's Finance and Budget Division (FBD) will conduct informational sessions/trainings to demonstrate how S&T Analytical Tracking System (STATS) can be used to track project information to ensure policies and procedures are being followed, as well as provide clear expectations of when to use the terms "program," "project," and "activity." In October 2023, S&T's FBD initiated corrective actions to identify and correct inaccuracies and inconsistencies between the Federal Financial Management System and STATS data, and by January 2024 had established a data cleansing team and began developing several data visualization tools. ECD: August 29, 2025.

Appendix C:
List of Programs and Projects within the Audit Scope

Table 1. Critical Infrastructure MCS Programs and Projects

No.	PEC	Program	Project
1	62-03-09-001 62-03-09-002 62-03-09-003	Explosives Detection (now Physical Security)	Mass Transit
2	62-03-18-001	Explosives Detection (now Physical Security)	Soft Target Crowded Places Security
3	63-03-02-001 63-03-02-002 63-03-02-101	Explosives Threat Assessment	Homemade Explosives Identification, Detection and Mitigation
4	65-09-06-002	Community and Infrastructure	Critical Infrastructure Resilience
5	65-09-07-001 65-09-07-002 65-09-07-003	CISRR	CISRR – Electromagnetic Pulse and Geomagnetic Disturbance Resiliency
6	68-02-01-001	Countering Violent Extremism	Public Safety Violence Prevention
7	68-02-02-001 68-02-02-002	CISRR	CISRR – Public Safety and Violence Prevention
8	68-03-01-001	Physical Security	Soft Target, Vehicle, School Safety
9	68-03-03-001 68-03-03-002 68-03-03-003	CISRR	CISRR – Soft Target Physical Security

Source: STATS and S&T officials

Table 2. Innovation and Collaboration Critical Infrastructure Centers of Excellence

No.	PEC	Program	Project (Center of Excellence)
1	40-01-10-001	DHS Centers	Awareness and Localization of Explosives-Related Threats (ALERT) - Emeritus[28]
2	40-01-14-001	DHS Centers	National Counterterrorism Innovation, Technology, and Education Center (NCITE)
3	40-01-17-001	DHS Centers	Critical Infrastructure and Resilience Institute (CIRI)
4	40-01-24-001	DHS Centers	National Counterterrorism Innovation, Technology, and Education Center (NCITE)
5	40-01-25-001	DHS Centers	Soft-Target Engineering to Neutralize the Threat Reality (SENTRY)

Source: STATS and S&T officials

[28] Emeritus Centers of Excellence are centers that have completed the term of their cooperative agreement.

Appendix D:
S&T CISRR Focus Area Descriptions

Focus Area 1 – Special Event Assessment Rating Planning Tools
This focus area aims at enhancing physical security at special events by providing assistance, such as explosive detection canine teams, cyber risk assessments, venue screening and field intelligence teams, and air security and tactical operations support.

Focus Area 2 - Electromagnetic Pulse and Geomagnetic Disturbances
Electromagnetic Pulse and Geomagnetic disturbance events could heavily impact large-scale infrastructure by disrupting or permanently damaging critical electrical components and systems. This focus area aims at improving the understanding of the effects of these events on communications infrastructure through research and delivering this information to critical infrastructure owners and operators.

Focus Area 3 - Position, Navigation, and Timing Capabilities
U.S. critical infrastructure depends on reliable positioning, navigation, and timing capabilities and any disruption or damage of these services could send cascading effects throughout the infrastructure networks — including safety-of-life issues and complete system failure. This focus area aims at developing various methods, such as approaches, best practices, and solutions that ensure the continued resilience of critical infrastructure if a position, navigation, and timing event were to occur.

Focus Area 4 - Public Safety and Violence Prevention/Soft Target Security
Soft targets and crowded places are at risk of foreign and domestic terrorist attacks. This focus area aims at improving security efforts related to the prevention, protection, response, and mitigation of potential attacks to soft targets and crowded places, including improving capabilities in countering improvised explosive devices.

Focus Area 5 - Security Testing Capabilities for Telecommunications Equipment, Industry Control Systems, and Open-Source Software
This includes telecommunications networks to factories, power plants, water systems, industrial facilities, and other critical infrastructure that are at risk of cybersecurity attacks. This focus area aims at improving capabilities related to threats to telecommunications networks, cybersecurity, and open-source software.

Appendix E:
S&T's BPF Processes and Decision Points

BPF Processes and Decision Points

Phase	Process	Decision Points
Understand Needs	1: Collect Customer Needs	D1: S&T Gap/Need Prioritization
	2: Gap Decomposition and Customer Validation	D2: Customer Validates Refined Gap/Need and Priority
Apply a Deliberate Approach to Addressing Needs	3: Define Solution Approaches	D3: Customer Determines Viability of Solution Approaches
	4: Business Case Analysis	D4: Customer Confirms/Selects Solution Path
	5: Project Pitch	D5A: S&T Executive-Level Project Approval D5B: Customer Contributes Resources
Execute Efficiently and Effectively	6: Project and Resource Planning	D6: Customer Agrees to Move Forward with Project Plan
	7: Solution Execution and Assessment	D7: Customer Accepts Solution
	8: Solution Delivery	None
	9: Post-Delivery Close-out	None

Source: S&T's *Understanding S&T's Business Process Flow*

Appendix F:
Major Contributors to This Report

The Office of Audits major contributors to this report are Yesi Starinsky, Audit Director; Ruth Blevins, Audit Director; Douglas Campbell, Audit Manager; John Schmidt, Auditor-in-Charge; Lauren Bullis, Auditor; Rebecca Hetzler, Auditor; Tanya Suggs, Auditor; Kevin Dolloson, Communications Analyst; and Nadine F. Ramjohn, Independent Reference Reviewer.

The Office of Innovation major contributors are Gaven Ehrlich, Supervisory Program Analyst and Joseph Welton, Program Analyst.

Appendix G:
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 Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

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