



OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

INSPECTION REPORT

DOE-OIG-25-11

December 2024

**ALLEGATIONS OF MANAGEMENT
CONCERNS AT THE DEPARTMENT OF
ENERGY'S OFFICE OF INTELLIGENCE
AND COUNTERINTELLIGENCE**



Department of Energy
Washington, DC 20585

December 30, 2024

MEMORANDUM FOR THE DIRECTOR, OFFICE OF INTELLIGENCE AND
COUNTERINTELLIGENCE

SUBJECT: Inspection Report: *Allegations of Management Concerns at the Department of Energy's Office of Intelligence and Counterintelligence*

The attached report discusses our inspection of allegations of management concerns at the Department of Energy's Office of Intelligence and Counterintelligence (DOE-IN). We substantiated the allegation that Department Headquarters' Sensitive Compartmented Information Facilities in the Forrestal Building did not meet U.S. Intelligence Community requirements. These issues occurred, in part, because DOE-IN did not develop and implement a formal corrective action plan with a strategic approach to improve Sensitive Compartmented Information Facilities compliance at Department Headquarters, including the necessary resources to implement the corrective action plan. We did not substantiate the allegation that DOE-IN authorized a contractor employee to procure a contract for a congressionally directed review of DOE-IN's Counterintelligence Program. Further, while we substantiated the allegation that DOE-IN has contractor employees conducting inspections of DOE-IN's Counterintelligence Program, we determined that the use of contractor personnel to conduct these inspections is not against DOE-IN policy. This report contains two recommendations that, if fully implemented, should help ensure that the Department maintains its Sensitive Compartmented Information Facilities in compliance with U.S. Intelligence Community requirements. Management fully concurred with our recommendations.

We conducted this inspection from October 2023 through October 2024 in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation* (December 2020). We appreciated the cooperation and assistance received during this inspection.

A handwritten signature in black ink, appearing to read "Anthony Cruz", is located in the lower right quadrant of the page.

Anthony Cruz
Assistant Inspector General
for Inspections, Intelligence Oversight,
and Special Projects
Office of Inspector General

cc: Deputy Secretary
Chief of Staff

DOE-OIG-25-11



Department of Energy Office of Inspector General

Allegations of Management Concerns at the Department of Energy's Office of Intelligence and Counterintelligence (DOE-OIG-25-11)

WHY THE OIG PERFORMED THIS INSPECTION

The Office of Inspector General received an anonymous complaint alleging that: (1) Department of Energy Headquarters' Sensitive Compartmented Information Facilities (SCIF) in the Forrestal Building have been out of compliance with U.S. Intelligence Community requirements; (2) the Office of Intelligence and Counterintelligence (DOE-IN) authorized a contractor employee to procure a contract for a congressionally directed review of DOE-IN's Counterintelligence (CI) Program, which may have been a conflict-of-interest violation; and (3) DOE-IN has contractor employees conducting inspections of DOE-IN's CI Program.

We initiated this inspection to determine the facts and circumstances regarding the alleged management concerns at DOE-IN.

What Did the OIG Find?

We substantiated the allegation that Department Headquarters' SCIFs in the Forrestal Building did not meet U.S. Intelligence Community requirements. Specifically, we found that SCIF reaccreditations, technical security reviews, and self-assessments were not conducted for some SCIFs occupied by DOE-IN. These issues occurred, in part, because DOE-IN did not develop and implement a formal corrective action plan with a strategic approach to improve SCIF compliance at Department Headquarters, including the necessary resources to implement the corrective action plan. To its credit, we noted that DOE-IN began making progress in calendar year 2023. In addition, we did not substantiate the allegation that DOE-IN authorized a contractor employee to procure a contract for a congressionally directed review of DOE-IN's CI Program; therefore, we did not substantiate the allegation that there was a conflict-of-interest violation. Further, while we substantiated the allegation that DOE-IN has contractor employees conducting inspections of DOE-IN's CI Program, we determined that the use of contractor personnel to conduct these inspections is not against DOE-IN policy. DOE-IN leadership approves the selection of the lead inspector and provides Federal oversight for CI Program inspections.

What Is the Impact?

Noncompliance with U.S. Intelligence Community security requirements, which ensure that critical safeguards are fully implemented, may result in degradation of the security posture for SCIFs, potentially exposing highly classified national security information.

What Is the Path Forward?

To address the issues identified in this report, we have made two recommendations that, if fully implemented, should help ensure that the Department maintains its Headquarters' SCIFs in compliance with U.S. Intelligence Community requirements.

BACKGROUND

The Department of Energy's Office of Intelligence and Counterintelligence's (DOE-IN) mission is to protect vital national security and technologies by leveraging the Department's scientific and technological expertise in support of policymakers and national security missions in defense, homeland security, cybersecurity, intelligence, and energy security. DOE-IN is responsible for all intelligence and counterintelligence (CI) activities throughout the Department's complex, including nearly 30 intelligence and CI offices throughout the Nation.

The U.S. Intelligence Community consists of organizations that include, but are not limited to, the Department and the Central Intelligence Agency. The Intelligence Reform and Terrorism Prevention Act of 2004 establishes the Office of the Director of National Intelligence as the head of the U.S. Intelligence Community. The Office of the Director of National Intelligence oversees and implements the National Intelligence Program, which includes standards and processes used to ensure consistency within the U.S. Intelligence Community. For the Department, DOE-IN has overall responsibility for ensuring that Sensitive Compartmented Information Facilities (SCIFs) meet National Intelligence Program standards.

In September 2022, the Office of Inspector General received an anonymous complaint alleging that: (1) Department Headquarters' SCIFs in the Forrestal Building have been in noncompliance with U.S. Intelligence Community security requirements; (2) DOE-IN authorized a contractor employee to procure a contract for a congressionally directed review of DOE-IN's CI Program, which may be a conflict-of-interest violation; and (3) DOE-IN has contractor employees conducting inspections of DOE-IN's CI Program. According to the complaint, these inspections are required to be led by a Federal employee, but a contractor employee has been the lead inspector "for years." We initiated this inspection to determine the facts and circumstances regarding the alleged management concerns at DOE-IN.

SCIFs DID NOT MEET U.S. INTELLIGENCE COMMUNITY REQUIREMENTS

We substantiated the allegation that Department Headquarters' SCIFs in the Forrestal Building did not meet U.S. Intelligence Community requirements. Specifically, we found that SCIF reaccreditations, technical security reviews, and self-assessments were not conducted for some SCIFs occupied by DOE-IN in accordance with Intelligence Community Directive 705, *Sensitive Compartmented Information Facilities* (ICD 705), and its related implementing standards. These issues occurred, in part, because DOE-IN did not develop and implement a formal corrective action plan with a strategic approach to improve SCIF compliance at Department Headquarters, including the necessary resources to implement the corrective action plan. To its credit, we noted that DOE-IN began making progress starting in calendar year 2023.

Sensitive Compartmented Information Facilities Reaccreditations Not Conducted

Approximately 43 percent of SCIFs occupied by DOE-IN in the Forrestal Building at Department Headquarters were not reaccredited in accordance with required timeframes. A SCIF is defined by the National Institute of Standards and Technology as an area, room, group of rooms, buildings, or installation certified and accredited as meeting Director of National

Intelligence security standards for the processing, storage, and/or discussion of sensitive compartmented information (SCI). ICD 705 requires SCIFs to be accredited prior to being used for SCI purposes. A Letter of Accreditation is a formal statement on behalf of the Intelligence Community Element Head indicating that a facility has been designed, constructed, inspected, and certified for the protection of all SCI compartments, programs, or special activities in accordance with the provisions of ICD 705.

We found that approximately 43 percent of the SCIFs occupied by DOE-IN in the Forrestal Building at Department Headquarters were not reaccredited by the Designated Agency Official within the timeframes established by interim accreditation letters. Specifically, DOE-IN issued interim accreditations, valid for only 6 months, to 43 percent of the SCIFs. Interim accreditations can be issued by the Designated Agency Official to allow SCIFs to be used pending receipt of required documentation or a final inspection. However, the SCIFs were not reaccredited after the 6-month period expired. The interim accreditations for 29 percent of the SCIFs were due for review and reaccreditation approximately 4 years ago in March 2020 while 14 percent were due for review and reaccreditation in early December 2023. As of March 2024, DOE-IN had not provided documentation to us that the SCIFs have been reaccredited.

Technical Security Reviews Not Conducted

Approximately 43 percent of SCIFs had not had technical security reviews conducted in accordance with requirements. While specific requirements and timelines for these reviews are classified, technical security reviews, in general, ensure protection of SCI.

Self-Assessments Not Conducted

Annual self-assessments were not performed as required by Intelligence Community Technical Specification for ICD 705, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities* (IC Technical Specification), for more than half of the SCIFs reviewed. According to the IC Technical Specification, security officers shall conduct annual self-assessments to ensure the continued security of SCIF operations, to identify deficiencies, and to document corrective actions taken. The IC Technical Specification also requires results to be forwarded to the accrediting official and for copies to be retained by the security officer. During our review, we determined that approximately 57 percent of the SCIFs reviewed did not have required annual self-assessments performed for several years. Specifically, self-assessments for 43 percent of SCIFs were conducted in February 2020 but were not conducted again for over 3 years until December 2023 and February 2024. A self-assessment for approximately 14 percent of the SCIFs was last conducted in 2020, and as of February 2024, DOE-IN had not conducted the required self-assessments for these SCIFs.

Further, prior reviews by the Office of Enterprise Assessments (EA) of DOE-IN SCIFs identified longstanding significant and recurring issues pertaining to self-assessments. EA's February 2013 assessment found that DOE-IN had not documented surveys conducted or results for its Headquarters facilities from calendar year 2009 through calendar year 2011.

EA's September 2018 assessment also found that self-assessments for DOE-IN SCIFs at Headquarters had not been conducted annually, and the self-assessments lacked sufficient depth to ensure compliance with security requirements.

Lack of Formal Corrective Action Plans

These issues occurred, in part, because DOE-IN did not develop and implement a formal corrective action plan with a strategic approach to improve SCIF compliance at Department Headquarters, including the necessary resources to implement the corrective action plan. For example, EA's February 2013 assessment found that none of its November 2008 assessment findings pertaining to DOE-IN SCIFs were addressed through formal corrective action plans. In February 2024, DOE-IN officials told us that there have not been any corrective action plans regarding the EA assessments that were conducted in the past. However, DOE-IN officials notified us that they were aware of issues regarding inadequate SCIF documentation, backlog of SCIF self-assessments, and the lack of policy and guidance. DOE-IN officials informed us that they have been understaffed, which hindered DOE-IN's ability to conduct SCIF self-assessments. DOE-IN officials stated that DOE-IN is trying to make positive changes, including hiring more personnel, as well as working on updating reviews and required documentation for SCIFs. The officials also informed us that there was only a small number of staff that were responsible for all DOE-IN SCIF security for more than 90 SCIFs across the Department's enterprise, including the SCIFs in the Forrestal Building that were part of this inspection.

To its credit, we noted that DOE-IN made progress, including reaccrediting approximately 57 percent of SCIFs in 2023, updating 86 percent of SCIF self-assessments from November 2023 through February 2024, and creating standard operating procedures for all SCIFs in December 2023. A DOE-IN official also explained that a mechanism for developing and tracking corrective actions for SCIF self-inspections at Headquarters has been constructed. Finally, the official stated that DOE-IN is working with the Office of the Director of National Intelligence to improve SCIF compliance.

CONTRACTOR EMPLOYEE DID NOT PROCURE A FEDERAL CONTRACT

We did not substantiate the allegation that DOE-IN authorized a contractor employee to procure a Federal contract for a congressionally directed review of DOE-IN's CI Program. Therefore, we also did not substantiate the allegation that there was a conflict-of-interest violation. The complaint stated that a congressionally directed inspection was scheduled to take place during which DOE-IN would be assessed by an independent company that would also report its findings to Congress. We noted that this inspection was in reference to a congressionally directed action derived from the Intelligence Authorization Act for Fiscal Year 2021, which calls for the assessment of all Government agencies' CI programs.

We determined that contractor personnel did not procure the contract for the congressionally directed action to review DOE-IN's CI Program. Our discussions and review of procurement

documents found that the “contract” was a task order¹ through an Interagency Agreement with another Government agency. Federal officials executed the procurement documents for the acquisition of the contractor that conducted the assessment of DOE-IN’s CI Program. This included a Federal procurement official as the Contracting Officer for the Interagency Agreement and a senior Federal DOE-IN official as the Requesting Agency Program Official for the task order.

Additionally, we did not substantiate that there was a conflict-of-interest violation. A former DOE-IN official who was present during the time of the contractor selection and acquisition stated that DOE-IN’s CI Program did not employ any personnel from the contractor that conducted the assessment. Because we determined that only Federal personnel were involved in the procurement of the Interagency Agreement task order, we determined that this allegation was unsubstantiated.

COUNTERINTELLIGENCE INSPECTION PROGRAM

We substantiated the allegation that DOE-IN has contractor employees conducting inspections of DOE-IN’s CI Program; however, we determined that the use of contractor personnel to conduct CI inspections is not against DOE-IN policy. According to DOE-IN policy, *Counterintelligence Inspection Program* (DOE-IN policy), DOE-IN personnel provide requested support to DOE-IN leadership and the lead inspector. Per DOE-IN policy, DOE-IN personnel are defined as any person employed by DOE-IN, or an employee of a Department contractor or subcontractor working under the direction and control of DOE-IN. Additionally, there is no language in DOE-IN policy that prohibits contractor personnel from serving as lead inspectors. Further, DOE-IN leadership at the CI directorate level approves the selection of the lead inspector and provides Federal oversight for CI Program inspections.

During our review of relevant documentation such as prior reviews and policies, as well as interviews, we learned that the CI inspection teams consisted of DOE-IN Federal and/or contractor personnel. For example, a July 2023 inspection report had contractor personnel on the team, and oversight of that team was provided by a Federal DOE-IN employee. A contractor employee also served as the lead inspector for an August 2017 staff assistance visit. Additionally, a DOE-IN official informed us that oversight of all CI inspection reports undergoes three levels of review and approval by DOE-IN Federal leadership.

IMPACT

To ensure safeguards and procedures necessary to prevent the unauthorized disclosure of SCI and other classified national security information in SCIFs, a life-cycle process of continuous monitoring and evaluations, periodic re-evaluations, and document reviews is required. These evaluations include, among other things, ensuring that: (1) accreditation standards are met, and (2) technical security reviews and annual self-inspections are conducted to ensure the continued

¹ According to Federal Acquisition Regulation 16.501-1, Definitions, a task order contract is defined as a contract for services that does not procure or specify a firm quantity of services (other than a minimum or maximum quantity) and that provides for the issuance of orders for the performance of tasks during the period of the contract.

security of SCIF operations. Noncompliance with U.S. Intelligence Community security requirements, which ensure that these critical safeguards are fully implemented, may result in degradation of the security posture for SCIFs, potentially exposing highly classified national security information.

RECOMMENDATIONS

We recommend that the Director, DOE-IN:

1. Develop a formal corrective action plan with a strategic approach to address the compliance issues for DOE-IN SCIFs at Department Headquarters and to help prevent recurrences with: (a) timely accreditations; (b) technical security reviews and self-assessments in accordance with requirements; and (c) the necessary resources for DOE-IN to implement the corrective action plan; and
2. Implement and track the corrective actions to completion to ensure that SCIFs meet U.S. Intelligence Community requirements.

MANAGEMENT RESPONSE

Management fully concurred with our recommendations and provided corrective actions taken, and in process, that will be completed by December 31, 2025. According to DOE-IN, it is developing a Security Division Inspection Program to ensure that technical security reviews and self-assessments are conducted in accordance with Intelligence Community Directives, and it has allocated additional Federal and contractor staff to support this effort. Additionally, DOE-IN stated that it has already developed and implemented an interim Issue Management Program to effectively track all findings and deficiencies involving Department-accredited SCIFs and to ensure corrective actions are developed and implemented.

Management comments are included in Appendix 2.

INSPECTOR COMMENTS

Management's comments and corrective actions are responsive to our recommendations.

Appendix 1: Objective, Scope, and Methodology

OBJECTIVE

We initiated this inspection to determine the facts and circumstances regarding the alleged management concerns at the Department of Energy's Office of Intelligence and Counterintelligence (DOE-IN).

SCOPE

The inspection was performed from October 2023 through October 2024. We conducted the inspection at Department Headquarters in Washington, DC. The scope was limited to the facts and circumstances regarding the alleged management concerns at DOE-IN from January 2013 through December 2023. The inspection was conducted under Office of Inspector General project number S23HQ020.

METHODOLOGY

To accomplish our inspection objective, we:

- Identified and reviewed applicable criteria (i.e., laws, regulations, Department directives, as well as policies and procedures) related to the allegations;
- Held discussions with Federal officials and subject matter experts from DOE-IN, the Office of Management, and the Office of Enterprise Assessments;
- Reviewed prior reports from the Office of Enterprise Assessments;
- Reviewed pertinent documentation concerning the accreditation and review of Sensitive Compartmented Information Facilities;
- Reviewed procurement documentation related to the fiscal year 2021 congressionally directed action to review DOE-IN's Counterintelligence Program; and
- Reviewed documentation related to DOE-IN's Counterintelligence Program inspections.

We conducted our inspection in accordance with the *Quality Standards for Inspection and Evaluation* (December 2020) as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions.

Management officials waived an exit conference on December 11, 2024.

Appendix 2: Management Comments



Department of Energy

Washington, DC 20585

December 10, 2024

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM:

Jay A. Tilden
JAY A. TILDEN

DIRECTOR

OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

SUBJECT:

ALLEGATIONS OF MANAGEMENT CONCERNS AT THE
DEPARTMENT OF ENERGY'S OFFICE OF INTELLIGENCE AND
COUNTERINTELLIGENCE (S23HQ020)

Thank you for the opportunity to review and comment on the subject draft report. The Office of Intelligence and Counterintelligence (DOE-IN) appreciates the auditors' audit work and concurs with the two recommendations.

The attachment to this memorandum details actions planned or already taken by the Office of Intelligence and Counterintelligence.

If you have any questions regarding this response, please contact Nancy Checklick, Chief of Staff, Office of Intelligence and Counterintelligence, 202-586-1789.

Enclosure

Appendix 2: Management Comments

Enclosure

Management Response
OIG Draft Report:
Allegations of Management Concerns at the Department of Energy's
Office of Intelligence and Counterintelligence
(S23HQ020)

Recommendation 1: We recommend that the Director, DOE-IN develop a formal corrective action plan with a strategic approach to address the compliance issues for DOE-IN SCIFs at Department Headquarters and to help prevent recurrences with: (a) timely accreditations; (b) technical security reviews and self-assessments in accordance with requirements; and (c) the necessary resources for DOE-IN to implement the corrective action plan.

DOE Response: Concur. The Office of Intelligence and Counterintelligence, Security Division (IN-33), has already taken proactive steps to develop a plan to ensure compliance issues with DOE Accredited SCIFs have been addressed. As part of this plan, IN-33 is developing a Security Division Inspection Program to ensure technical security reviews and self-assessments are conducted in accordance with Intelligence Community Directives. Also, we allocated additional federal and contractor staff to support this effort.

Estimated Completion Date: March 31, 2025

Recommendation 2: We recommend that the Director, DOE-IN implement and track the corrective actions to completion to ensure that SCIFs meet U.S. Intelligence Community requirements.

DOE Response: Concur. The Office of Intelligence and Counterintelligence has already developed and implemented an interim Issues Management Program to effectively track all findings and deficiencies involving DOE Accredited SCIFs and ensure corrective actions are developed and implemented. We are working to revise the security management database to meet existing requirements across all security disciplines and will add an Issues Management portion to the new system. Since the beginning of FY24, we have completed over 100 corrective actions across the DOE enterprise and developed corrective action plans for all findings and deficiencies identified in the Enterprise Assessment for DOE-IN SCIFs. For example, all DOE Accredited SCIFs have been entered into the Office of the Director of National Intelligence SCIF Repository and updates are made as changes occur. All SCIF Accreditations for DOE-IN HQ SCIFs have been updated and new accreditations and/or interim accreditations have been issued.

Estimated Completion Date: December 31, 2025

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at 202-586-1818. For media-related inquiries, please call 202-586-7406.