OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

INSPECTION REPORT

DOE-OIG-20-24

January 2020

REVIEW OF THE OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE'S CLOSING OF CATEGORY A SECURITY INCIDENTS

Department of Energy
Washington, DC 20585

January 8, 2020

MEMORANDUM FOR THE DIRECTOR, OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

FROM: Jennifer L. Quinones
Assistant Inspector General
for Audits and Inspections
Office of Inspector General

SUBJECT: INFORMATION: Inspection Report on "Review of the Office of Intelligence and Counterintelligence's Closing of Category A Security Incidents"

BACKGROUND

The Department of Energy's Office of Intelligence and Counterintelligence (Intelligence) is responsible for all intelligence and counterintelligence activities throughout the Department's complex, including nearly 30 intelligence and counterintelligence offices nationwide. Intelligence contributes to national security by having the ability to leverage the Department's scientific and technological expertise in support of policymakers, as well as national security missions in defense, homeland security, cyber security, intelligence, and energy security.

Department Order 470.4B, *Safeguards and Security Program*, requires that Category A security incidents be closed in the Safeguards and Security Information Management System (SSIMS), the Department's master repository for facility clearances, contracts, surveys, and other safeguards and security issues that require resolution. Category A security incidents are incidents that meet a designated level of significance relative to the potential impact on the Department and/or national security, thereby requiring the notification and pertinent involvement of the cognizant security office (i.e., special nuclear material and nuclear material, all classified material, and Department security badges determined to be the target of theft, etc.). One of the objectives of the Order is to ensure that the occurrence of a security incident prompts the appropriate graded response, to include an assessment of the potential impacts, appropriate notification, extent of condition, and corrective actions.

The Office of Environment, Health, Safety and Security (Health and Safety) manages and oversees SSIMS, and uses the system to track and report safeguard and security issues that require resolution. Intelligence is responsible for ensuring that Category A security incidents are properly closed in SSIMS. During our previous inspection report, *Review of Allegations Against*

a Department of Energy's Office of Intelligence and Counterintelligence Senior Official, dated July 2018, we identified unrelated concerns regarding Intelligence's handling of security incidents. As such, we initiated this inspection to determine whether Intelligence closed Category A security incidents in SSIMS, as required.

RESULTS OF INSPECTION

We determined that Intelligence did not properly close Category A security incidents in SSIMS, as required. This occurred because Intelligence had an informal agreement with Health and Safety not to populate Category A security incidents into SSIMS. As a result, the Department may not have the capabilities to assess incident data for the purpose of reviewing and enhancing security policies, and providing technical incident and causal analysis expertise to site and program offices, as requested. As such, we made recommendations aimed at improving Intelligence's compliance with the Order.

Category A Security Incidents

We found that Intelligence did not properly close Category A security incidents in SSIMS, as required by the Order. We obtained a listing of Category A security incidents from Intelligence that had been reported to Intelligence from January 2015 through June 2018, which totaled 86 incidents. We then compared this listing to a SSIMS report provided by Health and Safety for the same period. We found that SSIMS did not contain any record of the 86 Intelligence Category A security incidents, and therefore, could not have been closed in accordance with the Order.

Informal Agreement

Intelligence did not close Category A security incidents in SSIMS in accordance with the Order because Intelligence had an informal agreement with Health and Safety not to populate Category A security incidents into SSIMS. We were told that this agreement had been established by a former Intelligence official who was reluctant to put Category A security incident information into SSIMS because the information could be sensitive (i.e., related to other external agencies or to foreign Governments) and there was a risk that the information could be compromised. However, a Health and Safety official told us that a process was in place to prevent entering sensitive information into SSIMS. We were unable to determine why the former Intelligence official chose not to use this process because he was no longer with the Department.

During our inspection, we also reviewed Intelligence's formal policy on reporting security incidents. IN Policy Document Number 703.1, *Reporting Incidents of Security Concern*, establishes the requirement that Category A security incidents be reported to Intelligence for adjudication. However, the policy does not mention the use of SSIMS.

On June 28, 2018, shortly before starting our inspection, Health and Safety issued a memorandum to Intelligence setting forth the established policy and procedures regarding incidents of security concern associated with sensitive programs. Specifically, the memorandum emphasized the requirements of Department Order 470.4B and the use of SSIMS for Category

A incidents. Additionally, we interviewed an Intelligence official during our inspection who stated that Intelligence should abide by the memorandum; however, Intelligence has not updated its internal policy and practices to reflect this.

Lack of Information

As a result of Intelligence not closing Category A security incidents in SSIMS, Health and Safety may not have the capabilities needed to assess incident data for the purpose of reviewing and enhancing security policies, and providing technical incident and causal analysis expertise to site and program offices, as requested. Furthermore, the lack of properly closing Category A security incidents prevents Health and Safety from handling the long-term management of security incidents, and does not serve as an effective Program Planning Management tool for enhancing site-specific implementation of security policies.

RECOMMENDATIONS

We recommend that the Director, Office of Intelligence and Counterintelligence:

1. Discontinue its informal agreement with the Office of Environment, Health, Safety and Security, and comply with the Office of Environment, Health, Safety and Security's policy and Department Order 470.4B, *Safeguards and Security Program*, regarding the use of the Safeguards and Security Information Management System for Category A security incidents, as required; and

2. Update the Office of Intelligence and Counterintelligence's IN Policy Document Number 703.1, *Reporting Incidents of Security Concern*, to be consistent with the Office of Environment, Health, Safety and Security's policy and Department Order 470.4B, *Safeguards and Security Program*, regarding the use of the Safeguards and Security Information Management System for Category A security incidents.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and indicated that corrective actions have been initiated to address the issues identified in the report. Specifically, management stated it had discontinued the informal agreement with the Office of Environment, Health, and Safety and Security, and is in the process of updating the internal policy on *Reporting Incidents of Security Concern* to be consistent with Departmental orders.

INSPECTOR COMMENTS

Management comments and corrective actions are responsive to our recommendations.

Management comments are included in Attachment 3.

cc: Chief of Staff
Associate Under Secretary for Environment, Health, Safety and Security

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

We conducted this inspection to determine whether the Office of Intelligence and Counterintelligence (Intelligence) closed Category A security incidents in the Safeguards and Security Information Management System (SSIMS), as required.

SCOPE

This inspection was conducted at the Department of Energy's James Forrestal Building Headquarters office, located in Washington, DC. The inspection was performed from July 2018 to August 2019 and focused on the closing of Category A security incidents in SSIMS from January 2015 through June 2018. This inspection was conducted under the Office of Inspector General project number S18IS007.

METHODOLOGY

To accomplish our objective, we:

- Reviewed relevant Federal laws and regulations and Department policies and procedures related to Category A security incidents;
- Interviewed relevant personnel in Intelligence and the Office of Environment, Health, Safety and Security concerning Category A security incidents closed in SSIMS;
- Obtained and reviewed Intelligence's practices, policies, and procedures concerning the handling of security violations;
- Determined if Intelligence had obtained a waiver to not close Category A security incidents in SSIMS;
- Reviewed relevant documents to determine why Intelligence was not closing Category A security incidents in SSIMS;
- Reviewed Intelligence's Category A security incident reporting records for the period of January 2015 through June 2018; and
- Reviewed and compared SSIMS information provided by the Office of Environment, Health, Safety and Security with information provided by Intelligence concerning Category A security incidents.

We conducted this inspection in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*. Those standards require that we plan and perform the inspection to obtain sufficient, and appropriate evidence to provide a reasonable basis for our conclusions and observations based on our inspection

objective. We believe that the evidence obtained provided a reasonable basis for our conclusions and observations based on our inspection objective. Accordingly, the inspection included tests of controls and compliance with laws and regulations to the extent necessary to satisfy the inspection objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our inspection. Finally, we partially relied on computer-processed data to satisfy our inspection objective. We conducted a limited reliability assessment by comparing computer-processed data to supporting information and deemed the data was sufficiently reliable.

The Office of Intelligence and Counterintelligence waived an exit conference on November 4, 2019.

PRIOR REPORT

Inspection on *Review of Allegations Against a Department of Energy's Office of Intelligence and Counterintelligence Senior Official* (DOE-OIG-18-39, July 2018). In July 2016, the Office of Inspector General received allegations that a senior Office of Intelligence and Counterintelligence official had inappropriately: (1) transmitted classified information on an unclassified system; (2) awarded Government contracts to friends; and (3) directed or influenced a contractor to hire a relative. We initiated the inspection to determine the facts and circumstances surrounding the allegations. The allegations were not substantiated. As such, there were no recommendations or suggested actions. However, during the course of the review, we identified concerns regarding the Office of Intelligence and Counterintelligence's handling of security incidents.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

October 18, 2019

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM: STEVEN K. BLACK
DIRECTOR
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

SUBJECT: Response to the Office of Inspector General Draft Inspection Report on "Review of the Office of Intelligence and Counterintelligence's Closing of Category A Security Incidents" (S18IS007)

The Department of Energy (DOE) Office of Intelligence and Counterintelligence (DOE-IN) appreciates the opportunity to review and comment on the subject draft report. DOE-IN acknowledges the Inspector General's concerns and commits to assuring DOE Headquarters and Field elements adhere to DOE Order 470.4B, *Safeguards and Security Programs*, policy and procedures.

DOE-IN agrees with the report's recommendations. In fact, DOE-IN has already started to implement changes in how we report Category A security incidents in the Safeguards and Security Information Management System (SSIMS) and we are revising our internal security policy to align with DOE Order 470.4B. DOE-IN's official response to the recommendations is in the enclosure.

The Office of Inspector General should direct any questions to Adrienne McCloud, Director of Security, Office of Intelligence and Counterintelligence at (202) 586-1127.

Enclosure

Management Response to Recommendations
IG Draft Report - Review of the Office of Intelligence and Counterintelligence's Closing of Category A Security Incidents (S18IS007)

Recommendation 1: Discontinue its informal agreement with the Office of Environment, Health, Safety and Security, and comply with the Office of Environment, Health, Safety and Security's policy and Department Order 470.4B, Safeguards and Security Program, regarding the use of the Safeguards and Security Information Management System for Category A security incidents, as required.

Management Response: Concur. DOE-IN has discontinued the informal agreement with the Office of Environment, Health, Safety and Security that had relieved DOE-IN of the need to enter incidents of security concern (IOSC) into SSIMS.

Completion Date: September 30, 2019

Recommendation 2: Update the Office of Intelligence and Counterintelligence's IN Policy Document Number 703.1, Reporting Incidents of Security Concern, to be consistent with the Office of Environment, Health, Safety and Security's policy and Department Order 470.4B, Safeguards and Security Program, regarding the use of the Safeguards and Security Information Management System for Category A security incidents.

Management Response: Concur. DOE-IN is in the process of updating the internal policy on Reporting Incidents of Security Concern to be consistent with Departmental orders.

Estimated Completion Date: March 31, 2020

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.