U.S. Department of Energy
Office of Inspector General
Office of Inspections and Special Inquiries

Inspection Report

Internal Controls Over Sensitive Compartmented Information Access for Selected Field Intelligence Elements

DOE/IG-0796 July 2008

Department of Energy
Washington, DC 20585

July 1, 2008

MEMORANDUM FOR THE DIRECTOR, OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Inspection Report on "Internal Controls Over Sensitive Compartmented Information Access for Selected Field Intelligence Elements"

BACKGROUND

As a member of the U.S. Government's Intelligence Community, the Department of Energy (DOE) serves as the premier technical intelligence resource in the areas of nuclear weapons, nonproliferation, energy, science, technology, and emerging threats. DOE accomplishes its intelligence mission by drawing from technical expertise located throughout the Department complex. This necessitates Department-affiliated personnel having access to sensitive compartmented information (SCI), which is a designation given to classified information derived from intelligence sources, methods, or analytical processes that are required to be handled through designated access control systems.

DOE's Office of Intelligence and Counterintelligence is responsible for granting SCI access authorization to DOE-affiliated personnel who need access to intelligence information. Individuals must have an active Top Secret or "Q" clearance to be granted and maintain SCI access authorization. The Office of Intelligence and Counterintelligence maintains "Lockbox," a database that it uses to track SCI access authorizations.

To complement a recent Office of Inspector General inspection of internal controls associated with individuals on a DOE Headquarters SCI access roster, we initiated a review of local Field Intelligence Elements that the Office of Intelligence and Counterintelligence maintains at several DOE sites in support of its intelligence mandate. These field sites have local SCI personnel databases, as well as local databases to control physical access systems, e.g., badge readers, for local SCI facilities. The objective of the inspection was to determine the adequacy of internal controls over access to intelligence information at two of these Field Intelligence Elements, Los Alamos National Laboratory (Los Alamos) and Sandia National Laboratories (Sandia).

RESULTS OF INSPECTION

We concluded that the Office of Intelligence and Counterintelligence and the subordinate Field Intelligence Elements at Los Alamos and Sandia did not have adequate administrative internal controls over their databases used to track SCI access authorizations. Based on our comparison of Lockbox and four local databases containing the names, authorizations, and facility accesses of Los Alamos and Sandia SCI access holders, we found that:

- The SCI personnel databases used by the Office of Intelligence and Counterintelligence, Los Alamos, and Sandia contained numerous errors, including incorrect database entries and failures to update information relevant to SCI access, which could lead to potentially serious security incidents;

- An individual physically accessed a Los Alamos SCI facility without escort after her SCI access authorization was terminated. Further, Los Alamos Field Intelligence Element officials did not report the security incident to appropriate Office of Intelligence and Counterintelligence officials. This incident illustrates the importance of maintaining correct, updated SCI databases; and,

- The Los Alamos Field Intelligence Element had not terminated the SCI access authorizations of 13 individuals whose personnel security clearances had been terminated up to 10 months previously.

We made several recommendations aimed at improving the Department's internal controls over SCI access authorizations.

MANAGEMENT REACTION

In responding to a draft of this report, management concurred with our recommendations and identified corrective actions taken, initiated, or planned. Management's verbatim comments are provided in Appendix C of the report.

Attachment

cc: Chief of Staff
Chief Health, Safety and Security Officer
Director, Office of Internal Review (CF-1.2)

INTERNAL CONTROLS OVER SENSITIVE COMPARTMENTED INFORMATION ACCESS FOR SELECTED FIELD INTELLIGENCE ELEMENTS

TABLE OF CONTENTS

Overview

INTRODUCTION AND OBJECTIVE

As a member of the U.S. Government's Intelligence Community, the Department of Energy (DOE) serves as the premier technical intelligence resource in the areas of nuclear weapons, nonproliferation, energy, science, and technology, as well as emerging nuclear threats. In addition to providing intelligence analyses, DOE offers specialized technology and operational support to both intelligence and law enforcement agencies.

DOE accomplishes its intelligence mission by drawing from technical expertise located throughout the Department complex, including the national laboratories. This necessitates Department-affiliated personnel having access to sensitive compartmented information (SCI), which is a designation given to classified information derived from intelligence sources, methods, or analytical processes that are required to be handled through designated access control systems.

DOE's Office of Intelligence and Counterintelligence is responsible for granting SCI access authorization to DOE-affiliated personnel who need access to intelligence information. Individuals must have an active Top Secret or "Q" clearance to be granted and maintain SCI access authorization. The Office of Intelligence and Counterintelligence maintains an SCI personnel database called Lockbox. This database directly "feeds" into and supports the official national SCI personnel database. The Office of Inspector General recently completed an inspection of internal controls associated with the 969 individuals on a DOE Headquarters SCI access roster. We identified issues with (1) individuals who had left the Department or had been debriefed from the SCI program remaining on the Department's SCI roster and (2) the execution of debriefing responsibilities by the Office of Intelligence and Counterintelligence.

To complement this inspection, we initiated a review of local Field Intelligence Elements that the Office of Intelligence and Counterintelligence maintains at several DOE sites in support of its intelligence mandate. These field sites have local SCI personnel databases, as well as local databases to control physical access systems, e.g., badge readers, for local SCI facilities. The objective of the inspection was to determine the adequacy of internal controls over access to intelligence information at two of these Field Intelligence Elements, Los Alamos National Laboratory

(Los Alamos) and Sandia National Laboratories (Sandia). According to Lockbox, as of October 1, 2007, there were 2,361 DOE SCI access holders at these facilities: 856 at Los Alamos and 1,505 at Sandia.

OBSERVATIONS AND CONCLUSIONS

We concluded that the Office of Intelligence and Counterintelligence and the subordinate Field Intelligence Elements at Los Alamos and Sandia did not have adequate administrative internal controls over their databases used to track SCI access authorizations. Based on our comparison of Lockbox and four local databases containing the names, authorizations, and facility accesses of Los Alamos and Sandia SCI access holders, we found that:

- The SCI personnel databases used by the Office of Intelligence and Counterintelligence, Los Alamos, and Sandia contained numerous errors, including incorrect database entries and failures to update information relevant to SCI access, which could lead to security incidents such as the one described below;

- An individual physically accessed a Los Alamos SCI facility without escort after her SCI access authorization was terminated. Further, Los Alamos Field Intelligence Element officials did not report the security incident to the required Office of Intelligence and Counterintelligence official; and,

- The Los Alamos Field Intelligence Element had not terminated the SCI access authorizations of 13 individuals whose personnel security clearances had been terminated up to 10½ months previously.

We note that in addition to the previously cited review of internal controls over SCI access authorizations on a DOE Headquarters access roster, other past reviews by the Office of Inspector General at Los Alamos and Sandia identified weaknesses in the internal controls intended to ensure that security clearances and access authorizations were terminated appropriately and expeditiously. A list of the associated reports is located at Appendix B.

Details of Findings

BACKGROUND

Individuals entering one or more SCI programs go through a series of in-processing actions. These actions are outlined in Director of Central Intelligence Directive (DCID) No. 6/1 (previously 1/19), "Security Policy for Sensitive Compartmented Information and Security Policy Manual." They include being sponsored, being administratively reviewed and approved by Office of Intelligence and Counterintelligence officials, receiving one or more video briefs, and reviewing Form 4414 (EF), "Sensitive Compartmented Information Nondisclosure Agreement." After reviewing the form, the individual signs and dates it to acknowledge an understanding of his/her security responsibilities. The individual also signs and dates the "Brief" block acknowledging receipt of the required briefings. DCID 6/1 states "Failure to sign an NdA [Nondisclosure Agreement] is cause for denial or revocation of existing SCI access. The NdA establishes explicit obligations on both the government and the individual signer for the protection of SCI."

When an individual no longer requires SCI access, the individual is to be debriefed on his/her continuing responsibility to safeguard SCI information. The individual then reviews the SCI Nondisclosure Agreement form and signs and dates the form in the "Debrief" block. The individual's SCI access authorization is considered to be terminated at this point.

We reviewed five databases. Los Alamos' and Sandia's local personnel databases were compared with Lockbox to determine if information relating to individuals with SCI access authorizations was accurate and consistent. The remaining two databases were associated with Los Alamos and Sandia SCI facility physical access systems and were reviewed to verify that personnel who were recently debriefed had not gained unescorted access to Laboratory SCI facilities.

DATABASE ISSUES

We found that the SCI personnel databases used by the Office of Intelligence and Counterintelligence, Los Alamos, and Sandia contained numerous errors, which could lead to security incidents such as the one described in the next section. Specifically, we identified 103 errors in Lockbox and local Los Alamos and Sandia personnel SCI access databases, including incorrect database entries and failures to update information relevant to SCI access. Of these identified errors:

- Six of the Lockbox errors were individuals who still had active SCI access authorizations even though they had been formally debriefed from SCI programs;

- Twenty of the Lockbox errors were individuals who were not entered, some for prolonged periods of time, to show that they were authorized to access SCI information;

- In several instances, Lockbox data boxes were inaccurately checked, preventing parties/organizations external to the Office of Intelligence and Counterintelligence from viewing the correct status of an individual's actual SCI access authorization; and,

- In some instances, the local databases contained inaccurate entries. For example, both Sandia and Los Alamos had wrong debriefing dates, and Sandia had instances where individuals whose SCI access requests had been denied or cancelled showed as being "Active" in the local SCI personnel database. (We did not find any evidence that any of these individuals had been SCI briefed or given unauthorized access to SCI information.)

We were told that some of these errors occurred when the Office of Intelligence and Counterintelligence combined four separate databases into one, Lockbox, in November 2006. We determined that Sandia submitted corrections in August 2007 and Los Alamos in October 2007. On December 4, 2007, we found that not all of the corrections had been made by the Office of Intelligence and Counterintelligence. However, at the conclusion of our inspection, all database issues had been corrected at all three locations.

In discussing the accuracy of Lockbox with an Office of Intelligence and Counterintelligence senior official, we were told that the office had experienced a 300 percent increase in workload the last 2 years with no increase in manpower. We were told that this had led to delays with inputting SCI access information, delays in correcting identified errors, and an inability to perform sufficient quality assurance/control on the database.

IMPROPER FACILITY ACCESS

We also found that an individual physically accessed a Los Alamos SCI facility without escort after her SCI access authorization was terminated. Further, Los Alamos Field Intelligence Element officials did not report the security incident to the required Office of Intelligence and Counterintelligence official.

On November 5, 2007, during our review of the Los Alamos SCI facility physical access system, we discovered that an individual who

was debriefed from the SCI program on November 8, 2006, gained unescorted access to a Los Alamos SCI facility on November 9, 2006, contrary to DOE policy. Procedures are supposed to be established to remove "an individual's authorization to enter an area when the individual is transferred, terminated, or the individual's access is suspended, revoked, or downgraded to a level below that required for entry." We immediately reported this previously undiscovered incident to Los Alamos officials. We were told that a Los Alamos Field Intelligence Element official subsequently initiated a telephonic conversation with the former employee. Reportedly, the individual told this official that she had returned to complete out-processing documentation. Another Los Alamos Field Intelligence Element official determined that the individual was able to gain access because her badge access authorization was not immediately removed from the Element's SCI facility physical access system. Her facility access was not terminated until November 13, 2006, and no one had reviewed whether she had accessed the facility in the intervening period of time.

We also determined that the Office of Intelligence and Counterintelligence Special Security Officer had not been informed of the security incident by the Los Alamos Field Intelligence Element, as required. After the Office of Inspector General identified the issue to the Special Security Officer, the Office of Intelligence and Counterintelligence requested additional information from Los Alamos. Los Alamos subsequently reported to the Special Security Officer that the security lapse occurred due to a series of events, to include the checklist executed for departing employees being reviewed and initialed as completed prior to collection of the employee's badge and deactivation of the employee's access in the badge reader system.

On January 14, 2008, the Office of Intelligence and Counterintelligence received an e-mail from Los Alamos stating that action was taken to ensure that no item on the checklist executed for departing employees is initialed as completed until the action has actually been completed. Based on this notification, the Office of Intelligence and Counterintelligence official said that all required actions had been completed.

LOS ALAMOS SCI ACCESS AUTHORIZATION TERMINATION

Finally, we found that the Los Alamos Field Intelligence Element had not terminated the SCI access authorizations of 13 individuals whose personnel security clearances had been terminated up to 10½ months previously. This appeared to be the result of the Element not having an effective means of being kept apprised of employee and personnel security clearance terminations. Specifically, the Element only had limited coordination with the Los Alamos entities handling employee and personnel security clearance terminations. In contrast, we noted that the Sandia Field Intelligence Element had taken actions to improve its integrated controls by establishing daily coordination with Sandia's Human Resources organization.

We also observed that this condition has the potential to result in the over-use of "administrative debriefings" by the Element. Administrative debriefings, which entail an authorized official annotating the SCI Nondisclosure Agreement with "Unavailable for Signature/Administrative Debrief," are only supposed to be used when all means to properly inform an individual of his/her continuing SCI access responsibilities have failed. The overuse of administrative debriefings has been cited in previous Office of Inspector General reports. We identified seven administrative debriefings at Los Alamos during this current review. Los Alamos contended that it only executed an administrative debriefing when it had exhausted identified methods to contact the individual to obtain a signature. While this may be true, we believe that Los Alamos might have more success actually debriefing individuals if it had more timely notification of individuals' departure.

A Los Alamos Field Intelligence Element official acknowledged that a week or a month could pass without his office being notified concerning the termination of an employee who had SCI access. He said that sometimes his office was not even notified of an individual's death. He also acknowledged that there were other Laboratory organizations that could assist with this issue. We believe that the Los Alamos Field Intelligence Element should coordinate with appropriate Laboratory organizations, such as the Human Resources and Personnel Security offices, in order to strengthen internal controls over SCI access authorizations.

RECOMMENDATIONS

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

1. SCI access authorization information is processed in Lockbox in an accurate, timely, and complete manner.

2. Lockbox and local databases are subjected to a periodic quality assurance/control regimen.

3. Los Alamos Field Intelligence Element officials receive refresher training concerning security incidents, with specific emphasis on security incident reporting.

4. The Los Alamos Field Intelligence Element establishes procedures with other Laboratory organizations to obtain timely notification concerning the termination of Laboratory personnel and personnel security clearances in order to ensure the timely termination of SCI access authorizations and minimize administrative debriefings.

MANAGEMENT COMMENTS

In comments on a draft of this report, the Office of Intelligence and Counterintelligence concurred with the report recommendations. Management identified corrective actions that have been or will be taken to address our recommendations. Management's comments are included in their entirety at Appendix C.

INSPECTOR COMMENTS

We consider management's comments to be generally responsive to our recommendations.

Appendix A

SCOPE AND METHODOLOGY

We conducted our inspection fieldwork between September and December 2007. We looked at the Field Intelligence Elements that were administered in association with Los Alamos and Sandia. We interviewed officials from the Office of Intelligence and Counterintelligence, Los Alamos, and Sandia regarding DOE and local SCI-related policy, standard operating procedures, paper files, and electronic databases. We reviewed applicable Director of Central Intelligence; National Nuclear Security Administration Service Center; Office of Intelligence and Counterintelligence; and Laboratory policies, procedures, electronic databases, and paper files.

We also compared five databases, three concerning SCI personnel access authorizations and two concerning physical access to SCI facilities; reviewed relevant Field Intelligence Element-related SCI personnel data entries; and in the case of SCI facility access, conducted a judgmental sample involving recently debriefed SCI access authorized personnel. At Los Alamos, we reviewed 76 of 143 database files concerning SCI debriefed individuals and SCI facility access; and at Sandia, 100 of 195. During our inspection, we observed operations at Los Alamos and Sandia National Laboratory-New Mexico SCI facilities, and we reviewed data for both of these sites as well as for Sandia National Laboratory-California.

Also, pursuant to the "Government Performance and Results Act of 1993," we determined the Los Alamos and Sandia contractual performance measure processes did not address access control issues relating to the Field Intelligence Elements or their operations. However, the Office of Intelligence and Counterintelligence and DOE's Office of Independent Oversight evaluate a number of physical security topics that relate to Field Intelligence Element operations.

This inspection was conducted in accordance with the "Quality Standards for Inspections" issued by the President's Council on Integrity and Efficiency.

Appendix B

PRIOR REPORTS The following Office of Inspector General reports involved work related to this inspection:

- "Office of Intelligence and Counterintelligence Internal Controls Over the Department of Energy's Sensitive Compartmented Information Access Program" (DOE/IG-0790, March 2008);

- "Badge Retrieval and Security Clearance Termination at Sandia National Laboratory-New Mexico" (DOE/IG-0724, April 2006); and,

- "Security and Other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory" (DOE/IG-0677, February 2005).

Department of Energy
Washington, DC 20585

JUN 16 2008

MEMORANDUM FOR: CHRISTOPHER R. SHARPLEY
DEPUTY INSPECTOR GENERAL FOR
INVESTIGATIONS AND INSPECTIONS

FROM: ROLF MOWATT-LARSSEN
DIRECTOR
OFFICE OF INTELLIGENCE AND
COUNTERINTELLIGENCE

SUBJECT: Draft Inspection Report on "Internal Controls over Sensitive Compartmented Information Access for Selected Field Intelligence Elements" (S071S031)

Thank you for the opportunity to comment on the draft subject report. As previously mentioned, the Department of Energy Special Security Office workload increased 300% within the past five years. While the Office of Intelligence and Counterintelligence (IN) has replaced one DOE SSO employee that retired in January 2008, an additional FTE for a security specialist has been approved and should be filled by early FY 2009. This position will be focused on personnel security and will enhance IN's internal controls over the SCI program.

This office concurs with your recommendations and plans to take the following actions to remedy the identified deficiencies (see attachment).

For additional information, please contact Richard Perry, Acting Director of Security for the Office of Intelligence and Counterintelligence on 202-586-3897.

Attachment

Comments on Inspector General Draft Report
"Internal Controls over Sensitive Compartmented Information Access for Selected Field Intelligence Elements" (S071S031)

1. Recommendation:

SCI access authorization information is processed in Lockbox in an accurate, timely and complete manner.

Management Comment

Concur

The Office of Intelligence and Counterintelligence (IN) is committed to ensure changes to the Lockbox/Scattered Castles database will be made within three working days (name changes/briefing and debriefing dates/investigative information, etc.)

IN will conduct quarterly checks against the Department of Energy's Central Personnel Clearance Index (CPCI) database to ensure all DOE Sensitive Compartmented Information (SCI) holders maintain the required Q access.

The creation/advertisement of a new security specialist position within the Special Security Office will focus on personnel security issues/management.

IN has also instituted a second tier review of information going into the Lockbox/Scattered Castles database.

These actions have been implemented and will be ongoing.

2. Recommendation:

Lockbox and local databases subjected to a periodic quality assurance/control regimen.

Management Comment

Concur

IN has instituted quarterly checks with Headquarter Security Officers regarding Federal and contractor individuals that hold SCI access. IN will require field SSOs to review their information on SCI access holders quarterly to ensure all personnel have a current requirement.

IN is currently conducting a 100% review of Federal and contractor SCI holders against the CPCI database administered by the various Personnel Security Offices to ensure current Q access is in place.

In addition, IN is conducting a 100% inventory of all debriefed Federal and contactors that held SCI with DOE to ensure the Lockbox/Scattered Castles database contains accurate debriefing information pertaining to previous holders of SCI access.

This action will be completed by 31 December 2008.

3. Recommendation:

Los Alamos Field Intelligence Element officials receive refresher training concerning security incidents with specific emphasis on security incident reporting.

Management Comment

Concur

IN has discussed this issue with appropriate Los Alamos National Laboratory (LANL) Field Intelligence Element (FIE) personnel to ensure procedures for reporting security incidents are followed. At the time of this incident LANL did not feel that there was a compromise of information, however, notification to IN management should have been made.

This action is closed.

4. Recommendation:

The Los Alamos Field Intelligence Element establishes procedures with other Laboratory organizations to obtain timely notification concerning the termination of Laboratory personnel and personnel security clearances in order to ensure the timely termination of SCI access authorizations and minimize administrative debriefings.

Management Comment

Concur

To address this issue LANL has added a section to the LANL Departure Worksheet (institutional process) that reads:

13. Q cleared employee(s) holding SCI access must meet with IAT-1 Special Security Office (SSO) for processing.

In the LANL SCIF training plan, all employees gaining access to SCI at LANL must read and acknowledge that they have read and understand the provisions in our SCIF User's Guide which states "any changes to your employment status ...must be reported to the SSO Office for resolution because continued SCI access must be justified." This same reporting requirement is presented during the initial SCI indoctrination as well as during annual SCI refresher training for LANL employees.

The LANL FIE reports that they have reopened a dialogue with the Personnel Security Group to be notified of changes to LANL employee status in case an individual holds SCI access.

These actions have been accomplished. This action is closed.

IG Report No. DOE/IG-0796

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message clearer to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report, which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Judy Garland-Smith at (202) 586-7828.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page

http://www.ig.energy.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.