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

Inspection Report

Unauthorized Weapon Discharge and Related Security Policies and Procedures at Sandia National Laboratory-New Mexico

INS-O-08-01 **February 2008**

Department of Energy
Washington, DC 20585

February 28, 2008

MEMORANDUM FOR THE ADMINISTRATOR, NATIONAL NUCLEAR SECURITY ADMINISTRATION

FROM: Christopher R. Sharpley
Deputy Inspector General for Investigations and Inspections

SUBJECT: INFORMATION: Inspection Report on "Unauthorized Weapon Discharge and Related Security Policies and Procedures at Sandia National Laboratory-New Mexico"

BACKGROUND

The Department of Energy's Sandia National Laboratory-New Mexico (Sandia) is involved in a variety of research and development programs to enhance national security through technology. Sandia maintains a protective force that is trained and equipped to secure its facilities and operations. On October 24, 2006, a Sandia Security Police Officer (SPO) discovered what appeared to be a bullet hole in an exterior door on the rooftop of Building 6585 in a controlled security area at Sandia. This door allows access to SPO Post 580. Sandia did not have any report of a weapon discharge to account for the hole. Sandia conducted three internal investigations and concluded that the incident occurred on or about October 22, 2006. One Sandia investigation determined it was likely a .40 caliber round that went through the door, the same caliber used by the Sandia SPOs. However, Sandia could not positively identify who fired the round.

Concerns regarding the incident were raised to the Office of Inspector General. Therefore, we initiated an inspection to review security policies, procedures, and practices relevant to the circumstances surrounding the incident.

RESULTS OF INSPECTION

We found violations of security policies and procedures relevant to the bullet hole incident. Further, some of these violations may have contributed to Sandia's inability to pinpoint more details about the incident. Specifically, we found that around the time the incident is believed to have occurred:

- The alarms for the rooftop doors of Building 6585 were on "access mode" for extended periods ranging from about 24 hours to 37 hours, inconsistent with applicable policy. This condition precluded detection of entry and exit to the area; and,

- A Sandia SPO assigned to Building 6585 failed to verbally respond to three consecutive required radio post checks, and the Sandia protective force failed to react to the situation in accordance with applicable procedures.

In addition, we found other policy and procedural violations that were routinely occurring, to include:

- Central Alarm Station operators were not signing on to the alarm system when they came on duty, in violation of a Sandia Protective Force General Order. Logging on to the system creates an accountability record of who is responsible for the Central Alarm Station operations, to include alarms, radio checks, and dispatching; and,

- When alarms for the rooftop doors of Building 6585 were activated (set off), frequently there was not an immediate assessment of the cause of each alarm, in violation of Department policy. For our sample period, 32 percent of the 198 alarms activated were not assessed within 10 minutes. Further, 13 percent were not assessed for 1 hour or more, with the longest time period being 5 hours and 12 minutes.

Our findings were consistent with the findings of the previously mentioned Sandia internal investigations. None of these investigations made any recommendations for corrective actions; however, attached to one of the investigative reports was a corrective action narrative provided by Sandia protective force management. In addition, a security system review was conducted by Sandia management that resulted in the identification of performance deficiencies and procedural and administrative changes in protective force operating procedures. However, actions remained necessary to fully correct the specific issues we identified; therefore, we made several recommendations to management to ensure these issues are appropriately addressed and to further enhance site security.

MANAGEMENT REACTION

In comments on a draft of this report, management agreed with the factual accuracy of the report and its recommendations. Management's comments are included in their entirety at Appendix B. Management's comments did not include planned corrective actions with target completion dates; therefore, consistent with Department of Energy Order 221.3, "Establishment of Management Decisions on Office of Inspector General Reports," a management decision is required.

Attachment

cc: Chief of Staff
Manager, Sandia Site Office
Director, Policy and Internal Controls Management (NA-66)
Director, Office of Internal Review (CF-1.2)
Audit Liaison, Sandia Site Office

UNAUTHORIZED WEAPON DISCHARGE AND RELATED SECURITY POLICIES AND PROCEDURES AT SANDIA NATIONAL LABORATORY-NEW MEXICO

TABLE OF CONTENTS

Overview

INTRODUCTION AND OBJECTIVE

The Department of Energy's (DOE's) Sandia National Laboratory-New Mexico (Sandia) is involved in a variety of research and development programs to enhance national security through technology. Sandia's primary mission is to implement the Nation's nuclear weapons policies through research, development, and testing related to nuclear weapons. Sandia is administered by the National Nuclear Security Administration (NNSA) and is operated for NNSA by Sandia Corporation, a subsidiary of Lockheed Martin Corporation.

Sandia maintains a protective force that is trained and equipped to secure its facilities and operations. On October 24, 2006, a Sandia Security Police Officer (SPO) discovered what appeared to be a bullet hole in an exterior door on the rooftop of Building 6585 in Technical Area V at Sandia, which is a controlled security area. This door allows access to SPO Post 580, which is part of the security posture for Technical Area V. Sandia did not have any report of a weapon discharge to account for the hole. Sandia conducted three internal investigations and concluded that the incident occurred on or about October 22, 2006. One Sandia investigation determined it was likely a .40 caliber round that went through the door, the same caliber used by the Sandia SPOs. However, Sandia could not positively identify who fired the round.

Concerns regarding the incident were raised to the Office of Inspector General. Therefore, we initiated an inspection to review security policies, procedures, and practices relevant to the circumstances surrounding the incident.

OBSERVATIONS AND CONCLUSIONS

We found violations of security policies and procedures relevant to the bullet hole incident. Further, some of these violations may have contributed to Sandia's inability to pinpoint more details about the incident. Specifically, we found that around the time the incident is believed to have occurred:

- The alarms for the rooftop doors of Building 6585 were on "access mode" for extended periods ranging from about 24 hours to 37 hours, inconsistent with applicable policy. This condition precluded detection of entry and exit to the area; and,

- A Sandia SPO assigned to Building 6585 failed to verbally respond to three consecutive required radio post checks, and the Sandia protective force failed to react to the situation in accordance with applicable procedures.

In addition, we found other policy and procedural violations that were routinely occurring, to include:

- Central Alarm Station (CAS) operators were not signing on to the alarm system when they came on duty, in violation of a Sandia Protective Force General Order. Logging on to the system creates an accountability record of who is responsible for the CAS operations, to include alarms, radio checks, and dispatching; and,

- When alarms for the rooftop doors of Building 6585 were activated (set off), frequently there was not an immediate assessment of the cause of each alarm, in violation of DOE policy. For our sample period, 32 percent of the 198 alarms activated were not assessed within 10 minutes. Further, 13 percent were not assessed for 1 hour or more, with the longest time period being 5 hours and 12 minutes.

As stated previously, Sandia conducted three internal investigations in an attempt to determine when the bullet was fired through the door and by whom. A November 2006 investigation by the Sandia protective force did not identify the individual who fired the round. No report was written.

The second investigation was conducted by the Sandia Corporate Investigations office. A December 13, 2006, report concluded that "A lack of proper supervision, poor audit trails, lack of internal controls, no direct evidence, and a failure by the responsible individual(s) to come forward, has made an identification of the individual(s) responsible for the bullet hole in the door unattainable at this time." The report stated that "In summary, this has led to a serious breakdown in command and control."

The third investigation was performed by the Sandia Security Incident Management Program (SIMP). In a Report of Security Incident/Infraction dated March 22, 2007, SIMP concluded that "There is circumstantial evidence indicating [redacted] is the responsible individual for this incident. However, there is not enough physical evidence or testimonial evidence to allow SIMP to definitively determine responsibility for this incident."

We noted that, consistent with our findings, the three internal investigations identified violations of security policies and procedures. While none of the investigations made any recommendations for corrective actions, attached to the final SIMP

Report was a July 27, 2007, corrective action narrative provided by Sandia protective force management. This document stated that since the performance deficiencies were systemic in nature, the root cause was management failure and not any single point failure or individual operator action or inaction. Corrective actions identified included (1) the creation of an operations manager position with exclusive responsibility for protective force operations and (2) the institution of specific guidance on alarm acknowledgement and assessment, periodic alarm log reviews, and formal documentation of management's expectations for operational oversight of shift operations.

In addition, a security system review was conducted by Sandia management and resulted in the identification of performance deficiencies. In August 2007, Sandia management briefed the NNSA Sandia Site Office on procedural and administrative changes relating to CAS operators logging on to the alarm system, prescribed times for acknowledgement and assessment of alarms, and documenting the Daily Activity Report any time an alarm is not assessed in a timely manner. In addition, Sandia management is seeking clarification from NNSA on the requirement to immediately assess alarms due to Sandia's belief that "immediately" is a largely unachievable standard.

Details of Findings

DOOR ALARMS

We found that, around the time the bullet hole incident is believed to have occurred, the alarms for the rooftop doors of Building 6585 were on "access mode" for extended periods ranging from about 24 hours to 37 hours, inconsistent with applicable policy. This condition precluded detection of entry and exit to the area.

Building 6585 contains office space used by Sandia research groups, to include classified work. The rooftop of Building 6585 is used as part of a broader protection strategy that includes the prevention of theft or diversion of special nuclear material from other areas. DOE Manual 470.4-2, "Physical Protection," requires that all intrusion detection system sensors used to protect safeguards and security interests must annunciate directly to alarm stations when an alarm is activated and that alarm stations must provide a capability for monitoring and assessing alarms and initiating responses to safeguards and security incidents.

Sandia Protective Force Operations General Order 16, CAS/SAS Operations, states:

> When a sensor is in an "access mode," the sensor is **not** providing any alarm coverage. This mode is used when an alarm point is being used by authorized personnel or the area had been accessed.
>
> When a sensor is in a "secure mode," the sensor is providing both intrusion alarm and tamper alarm coverage. This mode is used when alarm coverage is required and **no** other compensatory measures are in place.

A Sandia official told us that it is Sandia's policy that doors are to be alarmed unless there is a need to access an area. We were also told that doors are not to remain in "access mode" for excessive periods of time and that, during non-operational hours, doors are to be placed in the "secure mode." We noted, however, that these requirements were not written into any of the Sandia Physical Security policies and procedures or Protective Force General Orders.

From our review of records, we determined that the alarm for the door with the bullet hole was turned to "access mode" at 11:31 PM on October 21, 2006, and not returned to "secure mode" until nearly 37 hours later. Also, there were three other door alarms on the same rooftop that remained in "access mode" for nearly 24 hours from October 22 to October 23, 2006.

Consistent with our finding, the SIMP Report of Security Incident/Infraction stated that:

> The alarms for the roof doors had been placed in "access mode" during the entire time in question. . . . This made it impossible to use alarm information to collaborate [sic] information obtained through the interviews with the officers who worked Post 580 during the time in question. It is not normal procedure to place building alarms in "access mode" for an extended period of time like this.

We were told by a Sandia management official that CAS operators had become accustomed to leaving the rooftop alarms in "access mode" to accommodate the SPO whose responsibility it was to frequently patrol the rooftop. We were also told that it had become apparent that SPOs felt that, since the building was continuously patrolled and the classified area was separately alarmed, there was no risk to putting the rooftop alarms in "access mode." However, Sandia management said that this behavior clearly did not meet protective force management expectations and that management did not endorse discretionary judgment in this respect. Sandia management said that they implemented corrective action.

SECURITY POST COMMUNICATION AND RESPONSE

We found that, around the time the bullet hole incident is believed to have occurred, a Sandia SPO assigned to Post 580 at Building 6585 failed to verbally respond to three consecutive required radio post checks, and the Sandia protective force failed to react to the situation in accordance with applicable procedures. Sandia General Order 16 in effect at the time of the incident stated that CAS operators shall "Conduct post security checks of Sandia Posts by performing a roll call using radio or phone to establish post and patrol status for welfare and location every half-hour on the half-hour." (Sandia General Order 16 has since been revised to require post security checks every hour.)

We determined that during the evening of October 22, 2006, a radio check at approximately 10:30 PM did not receive a verbal/ audio transmission response from Post 580. The radio was keyed (button pressed) for seven seconds, which did not constitute an effective response to the required radio post check. The next two consecutive required radio post checks at approximately 11:00 PM and 11:30 PM went completely unanswered.

Sandia General Order 16 also states that when there is "No Contact With a Post or Patrol," the CAS operator must notify the Field Lieutenant, dispatch personnel to search for the SPO, and attempt to contact the SPO via pager. In addition, the results must be documented on the Daily Activity Report, to include the reason for the lack of contact. However, we determined that:

- The CAS failed to notify the Field Lieutenant after the missed post checks at 10:30 PM, 11:00 PM, and 11:30 PM;

- When the CAS finally took action after the third missed post check at 11:30 PM, the CAS notified a roving SPO rather than the Field Lieutenant;

- In all three cases, the CAS failed to page Post 580. It was not until the roving SPO suggested paging the SPO at Post 580 that the CAS took this action at 11:36 PM, more than 1 hour after the first missed post check. Post 580 finally communicated with the Field Lieutenant at 11:51 PM; and,

- The missed radio checks were not documented on the Daily Activity Report for the evening of October 22, 2006. The Daily Activity Report showed one entry at 9:50 PM and the next entry at 1:17 AM on October 23, 2006.

The SIMP Report of Security Incident/Infraction and a November 22, 2006, letter to the protective force Manager titled "Post checks for the evening of October 22, 2006" raised the issue of missed radio checks involving Post 580. In addition, the SIMP Report also addressed the fact that there was nothing noted in the Daily Activity Report indicating that Post 580 did not respond to a scheduled post check. Neither of these documents contained recommendations for corrective action. The security system review conducted by Sandia management recognized that unanswered radio post checks were not properly resolved. However, the August 2007 Sandia management briefing to the Sandia Site Office did not specifically address corrective actions in the section on procedural and administrative changes.

CENTRAL ALARM STATION OPERATIONS

We found that CAS operators were not signing on to the alarm system when they came on duty, in violation of a Sandia Protective Force General Order. The Sandia protective force operates two CASs (North and South) that monitor alarms, closed circuit televisions, and operational communications with protective force personnel. Sandia General Order 16 requires each CAS operator, upon shift change, to log on to the Sandia Central Command System (SCCS). The order states that "A CAS operator must be logged onto the SCCS at all times." Logging on to the SCCS creates an accountability record of who is responsible for the CAS operations, to include alarms, radio checks, and dispatching.

We interviewed the two CAS operators who were on duty during the evening of October 22, 2006, when it was believed that the bullet

was fired into the door on the rooftop of Building 6585. Both operators said that they did not log on to the SCCS. We noted that the previously mentioned November 22, 2006, letter raised this issue; however, no recommendation for corrective action was made.

The two CAS operators further said that they had not logged on to the system in many years. We subsequently reviewed the SCCS log-on records for the month of October 2006. The records were divided between the North CAS and the South CAS. It appeared that the North CAS operators were logging on to the SCCS; however, there were no CAS operator entries for the South CAS.

The security system review conducted by Sandia management recognized that CAS operators were not logging on SCCS. The August 2007 Sandia management briefing to the Sandia Site Office addressed this issue in the section on procedural and administrative changes, stating that logging on to SCCS was mandatory for all CAS operators and that this would be verified by on-shift supervisors during random analysis of CAS records. In addition, we were told by a protective force official that the protective force has updated its General Order on CAS operations regarding the requirement to have CAS operators log on to the alarm system when coming on duty. If effectively implemented, these actions should resolve the CAS operators log on issue.

ALARM ASSESSMENT

We found that when alarms for the rooftop doors of Building 6585 were activated, there frequently was not an immediate assessment of the cause of each alarm, contrary to DOE policy. Specifically, DOE M 470.4-2, which was effective August 26, 2005, and was included in the Sandia contract under Appendix G, stated that:

> An effective method must be established for assessing all Intrusion Detection System (IDS) alarms . . . to determine the cause.
>
> (1) Alarms must be assessed immediately by either the PF [protective force] or by Central Alarm Station (CAS)/Secondary Alarm Station (SAS) personnel via Closed Circuit Television (CCTV).

We reviewed the door alarm assessment records for the rooftop of Building 6585 for the period October 15, 2006, through October 31, 2006. We determined that 64 of 198 alarms (32 percent) were not assessed within 10 minutes. Further, of the 64 alarms, 26 were not assessed for 1 hour or more, with the longest time period being 5 hours and 12 minutes.

Change 1 to DOE M 470.4-2 was issued March 7, 2006. Consistent with the original Manual, it required that intrusion detection system alarms used for the protection of Special Nuclear Material, classified matter, and Government property must be assessed immediately. We were told that, due to Sandia concerns regarding a series of changes to Department safeguards and security manuals, Change 1 was not incorporated into the Sandia contract until May 17, 2007.

We learned that Sandia management has since requested clarification of "the new policy" since "the new standard represents a largely unachievable standard." On July 18, 2007, Sandia management submitted an Implementation Plan for DOE M 470.4-2, Change 1, describing requirements that "cannot be implemented within 30 days." This plan sought clarification on the assessment of intrusion detection alarms, asking the question "What is DOE's definition of the term 'immediate?'"

We were told by a Sandia Site Office official that the requirement for immediate assessment is inconsistent with the response times identified in DOE M 470.4-4, "Information Security," for the protection of classified matter. We were also told that NNSA and the Site Office will recommend that this requirement be clarified during a rewrite of the Physical Protection Manual that is underway.

While we understand Sandia's concerns, we note that these concerns were not raised or resolved timely. The immediate assessment requirement was incorporated into Sandia's contract in 2005 and was supposed to be implemented within 30 days. Further, the alarm response times described in DOE M 470.4-4 for most assets are 15 and 30 minutes, yet we determined that in a number of cases alarms were not being assessed for well over 30 minutes. This could permit an undetected intruder to access or divert Government property or information.

We noted that the security system review conducted by Sandia management stated that any time an alarm is not assessed in a timely manner, it must be reported to the Shift Captain, investigated, and documented in the Daily Activity Report. We believe that, in addition to these actions, Sandia management needs to identify the root cause of the problem and develop policy to prevent future recurrence.

RECOMMENDATIONS

We recommend that the Manager, Sandia Site Office:

1. Seek timely resolution of policy concerns regarding alarm response times and then ensure timely implementation of the policy.

We also recommend that the Manager, Sandia Site Office, direct Sandia to:

2. Issue written policies and procedures for maintaining doors in "secure mode" during non-operational hours and for ensuring that building alarms are not placed in "access mode" for extended periods. Also, ensure these policies are followed.

3. Ensure that the Sandia Protective Force General Order requirements for addressing situations where there is "No Contact With a Post or Patrol" are followed, and that the Daily Activity Report is documented as required.

4. Ensure that CAS operators are logged on to the SCCS at all times, as required by Sandia Protective Force General Orders.

5. Identify the root cause of slow alarm response times and develop policy and procedures to prevent future recurrence of the problem.

MANAGEMENT COMMENTS

In comments on a draft of this report, management agreed with the factual accuracy of the report and its recommendations. Management noted that the "Physical Protection Manual" is in a re-write status and that appropriate items associated with the recommendations will be incorporated into the Manual. Management's comments are included in their entirety at Appendix B.

INSPECTOR COMMENTS

Management's comments did not include planned corrective actions with target completion dates; therefore, consistent with DOE Order 221.3, "Establishment of Management Decisions on Office of Inspector General Reports," a management decision is required.

Appendix A

SCOPE AND METHODOLOGY

The fieldwork for this inspection was concluded in December 2007. This inspection reviewed the alleged unauthorized weapon discharge incident and included:

- Review of CAS operations;
- Review of Sandia protective force orders;
- Review of Sandia investigation reports;
- Review of Sandia protective force alarm records and security reports; and,
- Interviews of Sandia protective force officials and SPOs.

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

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

February 12, 2008

MEMORANDUM FOR: Christopher R. Sharpley
Deputy Inspector General
for Investigations and Inspections

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comments to Draft Report on an Unauthorized Weapon Discharge; S07IS010; 2008-00159

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, "Unauthorized Weapon Discharge and Related Security Policies and Procedures at Sandia National Laboratory-New Mexico." We understand that this report is the result of your work from an allegation—and associated issues—related to an incident at the Laboratory that resulted in a bullet hole in an exterior door on the rooftop of Building 6585. While the incident occurred in October 2006 and there were several internal investigations into the incident, the IG conducted this inspection to review security policies, procedures, and practices relevant to the circumstances surrounding the incident.

NNSA agrees with the factual accuracy of the report and its corresponding recommendations. The Site Office, and others, is already working to obtain a clarification and/or resolution of the policy concerns regarding alarm response times. The Office of the Associate Administrator for Defense Nuclear Security and the Site Office have reached agreement that the Laboratory are in compliance and the Site Office is communicating this clarification to the Laboratory through the contractual process.

It is important to note that the "Physical Protection Manual" is in a review and re-write status. Appropriate items associated with these recommendations will be incorporated into the Manual during the review process and/or the RevCom process.

Should you have any questions about this response, please contact Richard Speidel, Director, Policy and Internal Controls Management.

cc: Patty Wagner, Manager, Sandia Site Office
Bill Desmond, Chief, Defense Nuclear Security
Karen Boardman, Director, Service Center

IG Report No. INS-O-08-01

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.