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

# Inspection Report

# Internal Controls over Accountable Classified Removable Electronic Media at Oak Ridge National Laboratory

INS-O-09-02

May 2009

**Department of Energy**
Washington, DC 20585

May 4, 2009

MEMORANDUM FOR THE MANAGER, OAK RIDGE OFFICE

FROM: Elise M. Ennis
Assistant Inspector General for Inspections

SUBJECT: INFORMATION: Inspection Report on "Internal Controls over Accountable Classified Removable Electronic Media at Oak Ridge National Laboratory"

BACKGROUND

The Department of Energy's Oak Ridge National Laboratory (ORNL) conducts cutting edge scientific research. ORNL utilizes removable electronic media, such as computer hard drives, compact disks, data tapes, etc., to store vast amounts of classified information. Incidents involving breakdowns in controls over classified removable electronic media have been a continuous challenge for the Department. The loss of even one piece of such media can have serious national security implications.

In 2004, the Department had a complex-wide "stand-down" of all activities using classified removable electronic media, and such media containing Secret/Restricted Data or higher classified data was designated "Accountable Classified Removable Electronic Media" (ACREM). As part of the stand-down, sites were required to conduct a 100 percent physical inventory of all ACREM; enter it all into accountability; and conduct security procedure reviews and training. Further, the Department implemented a series of controls, including conducting periodic inventories, utilizing tamper proof devices on ACREM safes, and appointing trained custodians to be responsible for the material. After performance testing and validation that the required accountability systems were in place, ACREM operations at ORNL were approved for restart on August 10, 2004.

We conducted a review at ORNL and associated facilities to determine whether ACREM is managed, protected, and controlled consistent with applicable requirements.

RESULTS OF INSPECTION

We found that:

- Eight pieces of Secret/Restricted Data media had not been identified as ACREM and placed into a system of accountability. Consequently, the items were not subject to all required protections and controls, such as periodic accountability inventories, oversight by a trained custodian, or storage in a designated ACREM safe. (However, the items were secured in safes approved for classified material.)

- Other required ACREM protections and controls were not implemented as follows: a tamper indicating device was not being used on an ACREM safe; records documenting when a certain safe was opened did not support that a purported inventory had been conducted; and a safe inventory had not been completed in a timely manner.

- A Personal Digital Assistant and a thumb drive, both capable of recording or transmitting data, were stored in a security area without an analysis to identify vulnerabilities and compensatory measures having been conducted, as required.

We also found that an ORNL Cooperative Research and Development Agreement partner had not disabled classified computer ports at the partner's site that were capable of writing classified information to external or removable media, as required.

We made several recommendations designed to enhance the security of ACREM, security areas, and computers.

MANAGEMENT REACTION

In responding to a draft of this report, management concurred with our recommendations. Management's comments are included in their entirety in Appendix C.

Attachment

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

# INTERNAL CONTROLS OVER ACCOUNTABLE CLASSIFIED REMOVABLE ELECTRONIC MEDIA AT OAK RIDGE NATIONAL LABORATORY

## TABLE OF CONTENTS

# Overview

## INTRODUCTION AND OBJECTIVE

The Department of Energy's (DOE's) Oak Ridge National Laboratory (ORNL), located in Oak Ridge, Tennessee, conducts cutting edge scientific research. ORNL, managed and operated by UT-Battelle, LLC, handles and stores some of the Nation's most sensitive information. DOE's Oak Ridge Office oversees the UT-Battelle contract.

ORNL utilizes removable electronic media, such as computer hard drives, compact disks, data tapes, etc., to store vast amounts of classified information. Incidents involving breakdowns in controls over classified removable electronic media have been a continuous challenge for DOE. The loss of even one piece of such media can have serious national security implications.

In 2004, the then DOE Deputy Secretary required a "stand-down" of all activities using classified removable electronic media at each DOE site in order to initiate enhanced security measures. DOE designated classified removable electronic media containing Secret/Restricted Data (S/RD) or higher classified data as "Accountable Classified Removable Electronic Media" (ACREM). DOE and its contractors were tasked to conduct a 100 percent physical inventory of all ACREM; enter all ACREM into an accountability system; and conduct security procedure reviews and ACREM custodian training. Recognizing the security risks associated with ACREM, DOE implemented a series of controls, including conducting periodic inventories, utilizing tamper proof devices on ACREM safes, and appointing trained custodians to be responsible for ACREM. After performance testing and validation that the required ACREM accountability systems were in place, the Deputy Secretary approved a restart of ACREM operations at ORNL on August 10, 2004.

We conducted a review at ORNL and associated facilities to determine whether ACREM is managed, protected, and controlled consistent with applicable requirements. Specifically, we inventoried virtually all the ACREM in accountability at ORNL, as well as a small sample of ACREM held by an ORNL Cooperative Research and Development Agreement partner. Further, we reviewed the contents of a sample of non-ACREM safes (safes identified as not containing ACREM and not under ACREM custodian control) at ORNL to determine if any ACREM materials were unidentified or uncontrolled.

## OBSERVATIONS AND CONCLUSIONS

At ORNL, we found that:

- Eight pieces of S/RD media had not been identified as ACREM and placed into a system of accountability. Consequently, the items were not subject to all required protections and controls, such as periodic accountability inventories, oversight by a trained ACREM custodian, or storage in a designated ACREM safe. (We noted that the eight items were secured in safes approved for the storage of classified material.)

- Other required protections and controls for ACREM were not implemented as follows: a tamper indicating device was not being used on an ACREM safe; records documenting when a certain safe was opened did not support that a purported inventory of ACREM had been conducted; and an ACREM safe inventory had not been completed in a timely manner.

- A Personal Digital Assistant (PDA) and a thumb drive, both capable of recording or transmitting data, were stored in a security area without an analysis to identify vulnerabilities and compensatory measures having been conducted, as required.

We also found that the ORNL Cooperative Research and Development Agreement partner, the United States Enrichment Corporation (USEC), had not disabled classified computer ports capable of writing classified information to external or removable media, as required. This was discovered at an offsite USEC facility.

To timely address specific security concerns, we notified ORNL officials of our findings during our fieldwork. The officials took prompt actions, including placing the eight pieces of ACREM into accountability; issuing two Incident of Security Concern reports; and, providing ACREM training to custodians. In addition, the Oak Ridge Office issued guidance to USEC to disable ports on its classified computers.

Appendix A to this report provides information regarding the scope and methodology of this inspection. Appendix B contains a list of related DOE Office of Inspector General and Government Accountability Office reviews regarding ACREM management, protection, and controls.

# Details of Findings

**ORNL ACREM ACCOUNTABILITY**

At ORNL, we found that eight pieces of S/RD media had not been identified as ACREM and placed into a system of accountability. As a result, the items were not subject to all required protections and controls, such as periodic accountability inventories, oversight by a trained ACREM custodian, or storage in a designated ACREM safe.

We noted that four of the eight items were found in designated ACREM safes that had been subject to inventories, but the custodians failed to identify the items. This called into question the quality of the inventories conducted. The remaining four items were found in non-ACREM safes used to store information classified as Secret and lower, which did not require periodic inventory. Of particular concern was a Bernoulli disk stored in a non-ACREM safe. An ORNL official informed us that the disk was placed in the non-ACREM safe approximately 8 to 10 years ago, meaning that the disk was not identified during the 2004 DOE-wide stand down that was supposed to have identified all ACREM.

As a result of our inspection, ORNL placed the eight pieces of ACREM into accountability, provided custodian training, and submitted two Incident of Security Concern reports to DOE's Office of Health, Safety and Security.

**ACREM PROTECTIONS**

We found that other required protections and controls for ACREM were not implemented at ORNL as follows.

**Tamper Indicating Devices**

A tamper indicating device was not being used on an ACREM safe. DOE Manual 470.4-4, "Information Security," requires that safes that store ACREM use tamper indicating devices, such as seals or "XO" series combination locks that would indicate possible unauthorized ACREM access. The XO series lock displays a sequential number that must be recorded each time the safe is accessed. XO series lock numbers out of sequence require a security notification. We determined that the custodian of an ORNL safe with an XO series lock had not recorded the lock's sequential number when the safe was accessed, and no other tamper indicating device was being used. The safe's custodian said he/she had never received tamper indicating device training and was not aware that a tamper indicating device was required. The custodian also said he/she was not aware of the requirement to record the lock's sequential number when the safe was accessed. After we identified this issue, we were told that ORNL applied tamper proof seals to the ACREM safe and provided training to the custodian.

**ACREM Record Discrepancy**

We also found that the records documenting when a certain safe was opened did not support that a purported inventory of ACREM had been conducted. According to DOE Manual 470.4-4, an inventory is to include a physical comparison of items in an ACREM safe against a current inventory listing. We compared the dates that inventories were supposedly completed with the opening numbers of the corresponding safe's XO series lock and determined that an inventory had purportedly been conducted on a date when there was no indication that the safe had been opened. As a result, ORNL issued the safe custodian who signed the inventory a security infraction for not opening the safe to conduct the inventory.

**ACREM Inventory**

Further, we found that an ACREM safe inventory had not been completed in a timely manner. Inventory controls are essential to ensure the protection and storage of ACREM. DOE Manual 470.4-4 requires that, at a minimum, ACREM inventories be conducted no less than once a year in the event of infrequent access. We determined that an inventory of one ACREM safe had not been completed in 16 months. ORNL was not aware that the inventory had not been conducted until we identified the concern. We were told that the custodian subsequently received training on ACREM inventory procedures.

**OTHER CONCERNS**

During our inspection, we identified other security issues as follows.

**Controlled Items**

We found that ORNL stored a PDA and a thumb drive, both controlled articles capable of recording or transmitting data, in a security area without conducting an analysis to identify vulnerabilities and compensatory measures, as required. DOE Manual 470.4-2, "Physical Protection," requires that controlled articles stored in a security area must be analyzed to identify vulnerabilities and to determine what countermeasures must be taken to prevent compromise. We determined that the PDA and the thumb drive contained classified information and had been confiscated by ORNL cyber security investigators. We were informed that an appropriate authorization to store these controlled items in the security areas was subsequently completed by ORNL.

**Computer Ports**

We found that USEC had not disabled classified computer ports capable of writing classified information to external or removable media, as required. In 2006, the then DOE Deputy Secretary required that the ports of all classified systems at each laboratory and other DOE facilities operating classified computer systems be disabled to protect against both insider and outsider threats. Further, DOE Manual 205.1-4, "National Security System Manual," requires that

ports and/or devices capable of writing classified information to removable or external media be protected from unauthorized use.

DOE provided classified information to USEC as part of a Cooperative Research and Development Agreement to develop centrifuge technology at an offsite facility. The Agreement required that USEC conform to all DOE regulations and requirements. However, we found that USEC had not disabled the ports on computers that contained information classified up to S/RD provided by DOE. We noted that DOE security officials previously had identified two separate findings regarding the ports. Subsequent to our raising this issue, we were provided a copy of a letter from USEC stating that it had taken action to comply with the requirement to disable the ports on classified computers.

**RECOMMENDATIONS**

We recommend that the Manager, Oak Ridge Office:

1. Review all safes at ORNL authorized to store classified information, whether or not designated to store ACREM, to ensure that all ACREM has been identified and placed into accountability;

2. Ensure that ACREM inventories at ORNL are conducted within required time frames and include a physical comparison of each item against a current inventory;

3. Ensure that proper authorization is obtained to store controlled items in a security area;

4. Given the diverse findings involving various individuals, ensure that employees who handle S/RD are provided appropriate training regarding ACREM accountability and other controls; and,

5. Ensure that ports on classified computers at USEC have been disabled.

**MANAGEMENT COMMENTS**

In comments on a draft of this report, the Department's Oak Ridge Office concurred with our recommendations. We have included management's comments in Appendix C.

**INSPECTOR COMMENTS**

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

# Appendix A

## SCOPE AND METHODOLOGY

Our review included ACREM activities at ORNL and associated facilities. The majority of our fieldwork was conducted from March through June 2008. It included interviews with DOE and contractor officials. Our document review and analysis and fieldwork activities included:

- DOE and local policies and regulations pertaining to ACREM;
- Selected samples of ACREM safes and other classified safes;
- Specific Site Security Plans;
- Local and independent ACREM assessment reports; and,
- Prior Office of Inspector General and other related reports.

We assessed compliance with the Government Performance and Results Act of 1993. Our review indicated that DOE established performance measures related to information security, although none specifically related to ACREM.

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 are prior related DOE Office of Inspector General reports:

- Special Inquiry Report to the Secretary, "Selected Controls over Classified Information at the Los Alamos National Laboratory" (November 27, 2006);

- "Destruction of Classified Hard Drives at Sandia National Laboratory-New Mexico" (DOE/IG-0735, August 3, 2006);

- "Security and Other Issues Related to Out-Processing of Employees at the Los Alamos National Laboratory" (DOE/IG-0677, February 22, 2005); and,

- "Internal Controls Over Classified Computers and Classified Removable Media at the Lawrence Livermore National Laboratory" (DOE/IG-0628, December 5, 2003).

The following are prior reports issued by the Government Accountability Office that had similar findings:

- "STAND-DOWN OF LOS ALAMOS NATIONAL LABORATORY Total Costs Uncertain; Almost All Mission-Critical Programs Were Affected but Have Recovered" (GAO-06-83, November 2005); and,

- "Nuclear Security: Lessons to Be Learned from Implementing NNSA's Security Enhancements" (GAO-02-358, March 2002).

DOE F 1325.8

United States Government **Department of Energy**
Oak Ridge Office

# memorandum

DATE: April 13, 2009

REPLY TO ATTN OF: FM-733:Miller

SUBJECT: **DRAFT INSPECTION REPORT ON "INTERNAL CONTROLS OVER ACCOUNTABLE CLASSIFIED REMOVABLE ELECTRONIC MEDIA AT THE OAK RIDGE NATIONAL LABORATORY" (SO81S005)**

TO: Elise M. Ennis, Assistant Inspector General for Inspections and Special Inquiries, IG-40, FORS

This is in response to your March 13, 2009, memorandum with attached draft report, subject as above. Following are the Oak Ridge Office's comments to the report recommendations as well as our comments on the accuracy of facts presented in the report:

**Recommendations: That the Manager, Oak Ridge Office:**

1. **Review all safes at ORNL authorized to store classified information, whether or not designated to store ACREM, to ensure that all ACREM has been identified and placed into accountability;**

**Management Response:**

Concur. Note that there was no evidence of loss or compromise of any classified information.

2. **Ensure that ACREM inventories at ORNL are conducted within required time frames and include a physical comparison of each item against a current inventory;**

**Management Response:**

Concur.

3. **Ensure that proper authorization is obtained to store controlled items in a security area;**

**Management Response:**

Concur. Although not ACREM, two controlled articles were discovered inside a GSA-approved repository located inside a Limited Security Area (LSA). ORNL, in conjunction with the ORNL Site Office, has a very formal process for allowing and approving controlled articles to be brought into a LSA. The formal process was not followed in this one instance. Follow-on Self-Assessments have not identified any similar failures to follow the formal process.

4. **Given the diverse findings involving various individuals, ensure that employees who handle S/RD are provided appropriate training regarding ACREM accountability and other controls; and**

**Management Response:**

Concur.

5. **Ensure that ports on all classified computers at USEC have been disabled.**

**Management Response**

Concur.

**COMMENTS ON ACCURACY OF FACTS:**

The following suggested clarifications are provided (in ***italicized text***):

Page 2, fourth paragraph:

We also found that the ORNL Cooperative Research and Development Agreement partner, the United States Enrichment Corporation (USEC), had not disabled classified computer ports capable of writing classified information to external or removable media, as required. ***This was discovered at an offsite USEC facility, not on the ORNL site.***

Signed

Judith M. Penry
Chief Financial Officer

cc:
George J. Malosh, SC-3, FORS
Gerald G. Boyd, M-1, ORO
Robert J. Brown, M-2, ORO
Pauline L. Douglas, OS-20, ORO
Johnny O. Moore, SC-10, ORO

IG Report No. INS-O-09-02

# 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.