



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

# Inspection Report

---

## Incident of Security Concern at the Y-12 National Security Complex



**Department of Energy**  
Washington, DC 20585

January 2, 2008

MEMORANDUM FOR THE SECRETARY

FROM:

*Greg Friedman*  
Gregory H. Friedman  
Inspector General

SUBJECT:

INFORMATION: Inspection Report on "Incident of  
Security Concern at the Y-12 National Security Complex"

BACKGROUND

The Y-12 National Security Complex (Y-12) in Oak Ridge, Tennessee, is a component of the Department of Energy's National Nuclear Security Administration. Y-12 is an integral part of the nuclear weapons complex and performs critical roles in strengthening national security. The success of Y-12's mission is dependent, in part, on the proper accreditation, use and control of classified and unclassified information systems.

In support of its mission, Y-12 maintains Limited Areas that employ physical controls to prevent unauthorized access to classified matter or special nuclear material. The Department has restrictions regarding what items may be taken into Limited Areas and the capabilities of those items. The Office of Inspector General received an allegation that unauthorized portable electronic devices (including laptop computers) were introduced into a Limited Area at Y-12 and that this breach in security was not properly reported. The objective of our inspection was to determine the facts and circumstances surrounding this matter.

RESULTS OF INSPECTION

Our inspection substantiated the allegation and identified additional concerns related to the incident. Specifically, we found that:

- On October 24, 2006, Y-12 personnel discovered that a contractor employee from the Department's Oak Ridge National Laboratory (ORNL) had brought an unclassified laptop computer into a Y-12 Limited Area without following proper protocols;
- Immediately thereafter, Y-12 cyber security staff did not properly secure the laptop computer, allowing the user to depart the Limited Area with the laptop computer. This was contrary to Department policy and prevented collection of the laptop computer as best evidence;



- Inconsistent with a 32-hour reporting requirement under the Department's Incidents of Security Concern Program, a written report of the incident was not made to the Headquarters Operations Center until six days after it was discovered; and,
- During Y-12 inquiries following the October 24, 2006, incident, it was determined that as many as 37 additional laptop computers may have been improperly introduced into the Limited Area by ORNL personnel in recent years. However, this was not reported to the Headquarters Operations Center immediately upon discovery. We noted that Y-12 included reference to these additional laptop computers in an updated investigative report submitted to Headquarters in May 2007.

During our review, we observed that information sharing between Y-12 and local counterintelligence officials could be improved. Specifically, four months after the incident, a key local counterintelligence officer was unaware of additional investigative files relating to the incident. We believe that the prompt and full communication of relevant information is critical, so that measures may be taken to address potential threats resulting from laptop computers having been taken on foreign travel.

We noted that, upon learning of the October 24<sup>th</sup> incident, the Manager of the Y-12 Site Office required that the involved individuals be removed from the Y-12 site and that their unclassified computer accounts be suspended. ORNL provided the laptop computers to Y-12 officials for a full security review and a forensic analysis. In addition, during the course of our inspection activities, officials from both sites notified us that they had initiated corrective plans and revisions to local security procedures. ORNL provided a detailed list of the corrective actions it either had initiated or was planning.

We made several recommendations designed to further enhance the security of information systems and responses to incidents of security concern.

#### MANAGEMENT REACTION

In responding to a draft of this report, management agreed with our recommendations and identified corrective actions taken, initiated or planned. Management comments were incorporated in the report, as appropriate, and are included in Appendix C. We consider the comments to be responsive to our recommendations. Due to the significance of the underlying security concerns, we are considering evaluating the adequacy of these corrective measures in the future.

Attachment

cc: Deputy Secretary  
 Administrator, National Nuclear Security Administration  
 Under Secretary for Science  
 Chief of Staff

Director, Policy and Internal Controls Management (NA-66)  
Director, Office of Internal Review (CF-1.2)  
Manager, Y-12 Site Office  
Manager, Oak Ridge Office  
Audit Liaison, Y-12 Site Office  
Audit Liaison, Oak Ridge Office

# INCIDENT OF SECURITY CONCERN AT THE Y-12 NATIONAL SECURITY COMPLEX

---

## TABLE OF CONTENTS

### **OVERVIEW**

Introduction and Objective .....	1
Observations and Conclusions .....	1

### **DETAILS OF FINDINGS**

Unauthorized Laptop Computer in Limited Area .....	3
Incident Response .....	3
Incident Reporting .....	3
Additional Unauthorized Laptop Computers .....	4
Communication .....	6

### **RECOMMENDATIONS** .....

7

### **MANAGEMENT COMMENTS** .....

7

### **INSPECTOR COMMENTS** .....

8

### **APPENDICES**

A. Scope and Methodology .....	9
B. Prior Reports .....	10
C. Management Comments .....	11

# Overview

---

## **INTRODUCTION AND OBJECTIVE**

The Y-12 National Security Complex (Y-12) in Oak Ridge, Tennessee, supports the Department of Energy's (Department) nuclear weapons program. Y-12 performs critical roles in strengthening national security and reducing the global threat from weapons of mass destruction. The success of Y-12's mission is dependent, in part, on the proper accreditation and use of classified and unclassified information systems.

The Office of Inspector General (OIG) received an allegation that unauthorized portable electronic devices (including laptop computers) were introduced into a Limited Area at Y-12 and that this breach in security was not properly reported. Limited Areas are secure work areas that employ physical controls to prevent unauthorized access to classified matter or special nuclear material. The Department has restrictions regarding what items may be taken into Limited Areas and the capabilities of those items. For example, modern laptop computers commonly have wireless transmission (WiFi) capability and infrared ports that can be used for high-speed data exchanges. Such capabilities are restricted or prohibited in secure environments without proper approvals, in order to protect against the disclosure of sensitive/classified information by the user or monitoring or intrusion by external threats. If an event occurs that threatens a security interest, it must be promptly and accurately reported to cognizant officials so that appropriate follow-up actions may be taken.

The Office of Inspector General initiated an inspection to determine the facts and circumstances surrounding the allegation.

## **OBSERVATIONS AND CONCLUSIONS**

Our inspection substantiated the allegation and identified additional concerns related to the incident. Specifically, we found that:

- On October 24, 2006, Y-12 personnel discovered that a contractor employee from the Department's Oak Ridge National Laboratory (ORNL) had brought an unclassified laptop computer into a Y-12 Limited Area without following proper protocols;
- Immediately thereafter, Y-12 cyber security staff did not properly secure the laptop computer, thereby allowing the user to depart the Limited Area with the laptop computer. This was contrary to Department policy and prevented collection of the laptop computer as best evidence;

- 
- Inconsistent with a 32-hour reporting requirement under the Department's Incidents of Security Concern Program, a written report of the incident was not made to the Headquarters Operations Center until six days after it was discovered; and,
  - During Y-12 inquiries following the October 24<sup>th</sup> incident, it was determined that as many as 37 additional laptop computers may have been improperly introduced into the Limited Area by ORNL personnel in recent years. However, this was not reported to the Headquarters Operations Center immediately upon discovery. We noted that Y-12 included reference to these additional laptop computers in an updated investigative report submitted to Headquarters in May 2007.

In addition, during our review, we observed that information sharing between Y-12 and local counterintelligence officials could be improved. Specifically, four months after the incident, a key local counterintelligence officer was unaware of additional investigative files relating to the incident. We believe that the prompt and full communication of relevant information is critical for responsible officials to develop an accurate and complete understanding of the facts and to determine the most effective path forward.

We noted that, upon learning of the October 24<sup>th</sup> incident, the Manager of the Y-12 Site Office required that the involved individuals be removed from the Y-12 site and their unclassified computer accounts suspended. ORNL provided all involved laptop computers to Y-12 officials for a full security review and a forensic analysis. In addition, during the course of our inspection activities, officials from both sites notified us that they had initiated corrective plans and revisions to local security procedures. ORNL provided a detailed list of the corrective actions it either had initiated or was planning. Due to the significance of the underlying security concerns, we are considering evaluating the adequacy of these corrective measures in the future.

The Office of Inspector General has completed several reviews related to information security and concerns regarding the ability of Department sites to protect both classified and unclassified information. Appendix B contains a list of related reviews, which in many instances found that security weaknesses were the result of failures to follow established Department or local policies and procedures.

## Details of Findings

---

### **UNAUTHORIZED LAPTOP COMPUTER IN LIMITED AREA**

We found that on October 24, 2006, Y-12 personnel discovered that a contractor employee from the Department's ORNL had brought an unclassified laptop computer into a Y-12 Limited Area without following proper protocols. On this date, cyber security staff had discovered this laptop computer with an unauthorized wireless capability in the Limited Area, identified the office and the computer's user, and reported the matter to a security official.

Department Manual 470.4-2, "Physical Protection," states that laptop computers capable of recording information and transmitting data wirelessly are considered controlled items and are not permitted in Limited Areas without special authorization. Special authorization is not given unless certain controls over the computers are exercised. These controls may include disabling the computers' internal microphone and wireless capabilities. In addition, local requirements at the Y-12 site stipulate that a laptop computer user seeking special authorization must electronically execute a Memorandum of Understanding to document full understanding of these rules and to accept responsibility that the requirements have been met. However, such a memorandum was not completed prior to the above laptop computer being brought into the Limited Area.

### **INCIDENT RESPONSE**

We found that immediately thereafter, Y-12 cyber security staff did not properly secure the laptop computer, thereby allowing the user to depart the Limited Area with the laptop computer. This was contrary to Department policy and prevented collection of the laptop computer as best evidence.

Department Manual 470.4-1, "Safeguards and Security Program Planning and Management," requires any person discovering a potential incident of security concern to make reasonable efforts to safeguard the security interests and to ensure evidence associated with the incident is not tampered with or destroyed. However, cyber security staff told us that once they discovered the unauthorized laptop computer inside the Limited Area, they had no local policies or procedures directing them how to properly safeguard the evidence associated with the incident. Therefore, the identified laptop computer user was permitted to leave the site with the laptop computer. It was up to an hour before the computer was retrieved.

### **INCIDENT REPORTING**

We determined that inconsistent with a 32-hour reporting requirement under the Department's Incidents of Security Concern Program, a written report of the incident was not made to the Headquarters



---

Operations Center until six days after it was discovered. The Department's Incidents of Security Concern Program required that a written report of the incident be submitted to the Headquarters Operations Center within 32 hours. Department Manual 470.4-1 states that officials have 24 hours to examine and document all pertinent facts and circumstances to determine if a security incident has occurred. If it is determined that a security incident has occurred, the severity and type must be categorized by an Impact Measurement Index numeric ranking within that same 24-hour period. Within eight hours following incident categorization, Department Form 471.1, "Security Incident Notification Report," must be submitted to the Headquarters Operations Center, which further processes and disseminates information regarding the incident.

We determined that a Department Form 471.1 reporting the October 24<sup>th</sup> incident was not sent to the Headquarters Operations Center until the morning of October 31, 2006. Department and contractor officials told us that they knowingly delayed submitting the required incident of security concern report because of uncertainty over whether ORNL or Y-12 would accept responsibility for formally reporting the incident and due to continually developing information. Y-12 ultimately accepted responsibility for reporting the incident.

Although a Department Form 471.1 was not submitted timely to the Headquarters Operations Center, we noted there were incident-related emails and phone calls to officials at the National Nuclear Security Administration (NNSA) Service Center in Albuquerque, New Mexico, and at Headquarters starting on October 25, 2006. However, none of these communications resulted in the required notification to the Headquarters Operations Center.

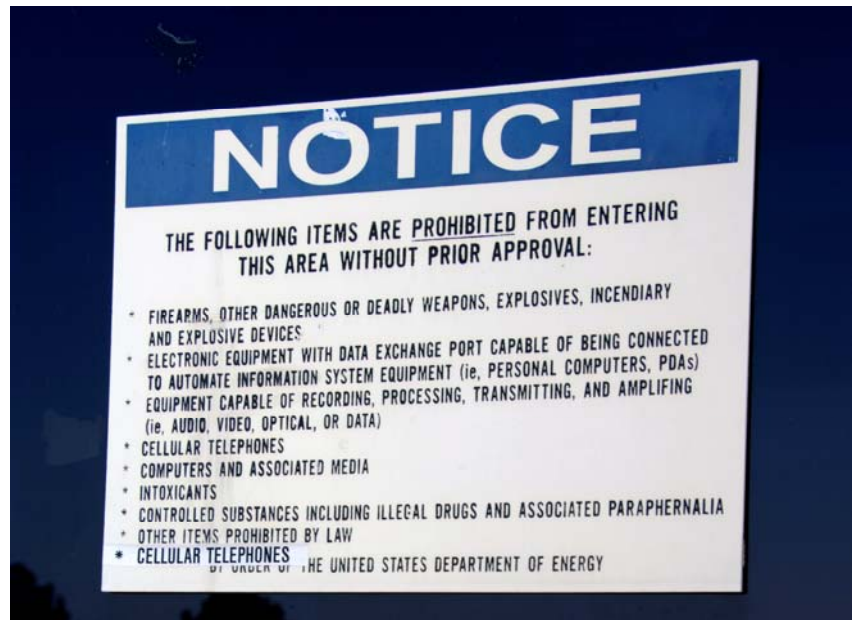
#### **ADDITIONAL UNAUTHORIZED LAPTOP COMPUTERS**

We found that during Y-12 inquiries following the October 24<sup>th</sup> incident, it was determined that as many as 37 additional laptop computers may have been improperly introduced into the Limited Area by ORNL personnel in recent years. However, this was not reported to the Headquarters Operations Center immediately upon discovery. We noted that Y-12 included reference to these additional laptop computers in an updated investigative report submitted to Headquarters in May 2007. In response to a draft of this report, management contended that it was appropriate to delay reporting this information until submission of its final investigative report provided to Headquarters in May 2007. However, we confirmed with a Headquarters security official that the additional laptop computers should have been reported upon discovery in

---

order to update and disseminate pertinent information about the security incident.

As noted earlier, according to Department policy, laptop computers capable of recording information and transmitting data wirelessly are not permitted in Limited Areas without special authorization. In addition, we observed that the entrance to the Limited Area had a sign (see below) that specifically prohibited entry of electronic equipment capable of recording, processing, and transmitting information without prior approval.



Sign posted outside the Limited Area

We determined that ORNL personnel allowed 38 laptop computers to be brought into the Limited Area without the required special authorizations and associated controls being implemented and without Memorandums of Understanding being executed. When interviewed, a computer security officer claimed a lack of knowledge regarding the established Y-12 policies and procedures on such laptop computers in the Limited Area.

### **Laptop Computer Analysis**

As stated in local ORNL guidance, portable electronic devices such as laptop computers are especially enticing targets for theft, unauthorized access, or espionage when traveling out of the country. Therefore, Y-12 officials conducted a review of the travel history of the laptop computers and found that 9 of the 38 laptop computers had been taken on foreign travel; 6 of those 9 had wireless capability; and 2 of those 6 had been to sensitive countries.

---

In addition, Y-12 submitted the 38 laptop computers to the Department's Cyber-Forensic Laboratory (CFL) for analysis. An examination of each laptop computer was conducted to determine if the computers contained classified information; if wireless connectivity had been made; and if any of the computers contained "malware" (a general term coined for a variety of malicious software). Their analysis concluded that the laptop computers did not contain classified information; that 26 of the 38 laptop computers had wireless communications capability; and that a majority of the computers contained malware. The CFL explained that while malware can have legitimate applications and is commonly found on most computers, some types have the potential to cause harmful, destructive or intrusive actions and can be used to capture a user's keystrokes to provide a means of obtaining unauthorized information. Senior ORNL and Y-12 officials, as well as an appropriate Federal agency, were informed of these issues. Department security offices conducted additional investigations, but did not identify a cyber security compromise. Consequently, the laptop computers were returned to their custodians and the Department categorized the incident as a physical security matter.

As a result of the violations of Department and local computer security procedures, the Manager of the Y-12 Site Office required that the involved individuals be removed from the Y-12 site and their unclassified computer accounts suspended. Following the completion of Y-12 mandated training, Y-12 reviewed ORNL reinstatement requests and reinstated facility access only for those ORNL employees deemed appropriate.

## **COMMUNICATION**

During our review, we observed that information sharing between Y-12 site and local counterintelligence officials could be improved. Through analysis of investigative materials, interviews, and internal communications, we discovered that four months after the incident, a key local counterintelligence officer was unaware of additional investigative files relating to the incident. Those files included information regarding potential conflicting statements made by the laptop computer user during the early stages of the October 24<sup>th</sup> incident investigation, the fact that the laptop computer and its user had left the area after the incident, and the specific identification of that laptop computer. We believe that the prompt and full communication of relevant information is critical for responsible officials to develop an accurate and complete understanding of the facts and to determine the most effective path forward.

---

## **RECOMMENDATIONS**

We recommend that the Manager, Oak Ridge Office:

1. Hold accountable those individuals who violated Department and site policies and procedures.
2. Conduct refresher training of all employees to ensure they understand the applicable requirements and their individual responsibilities with respect to the issues raised in this report.

We also recommend that the Manager, Y-12 Site Office:

3. Evaluate local policies and procedures to ensure they fully address the issues raised by our review.
4. Conduct refresher training of all employees to ensure they understand the applicable requirements and their individual responsibilities with respect to the issues raised in this report.
5. Conduct periodic reviews to ensure compliance with Department and local procedures on the use of laptop computers in Limited Areas.
6. Ensure that security incidents are reported in a timely and accurate manner in accordance with Department requirements.
7. Review information sharing procedures between site and local counterintelligence officials to ensure information is fully shared in a timely manner.

## **MANAGEMENT COMMENTS**

In comments on a draft of this report, the Department's Oak Ridge Office concurred with the recommendations and provided the OIG with a list of corrective actions that had been taken.

Management's corrective actions included the reassignment of some security duties and refresher training for all cleared personnel. We have included management's comments in Appendix C.

NNSA management stated that the recommendations were appropriate and provided an explanation of the actions taken to address our recommendations. These actions included updating policies and procedures related to laptop computers and conducting random inspections to test cyber security compliance. We have included management's verbatim comments in Appendix C.

---

**INSPECTOR  
COMMENTS**

We consider management's comments to be responsive to our recommendations. This report was reviewed for classification and handling.

# Appendix A

---

## **SCOPE AND METHODOLOGY**

The majority of our fieldwork was conducted from February through June 2007. It included interviews with Department and contractor officials and visits to the Y-12 Limited Area. Our document review and analysis included:

- Timeline of events associated with the incident;
- Security Incident Notification Report;
- Internal investigative reviews;
- Evidence/Property custody documents;
- Cyber-Forensic Laboratory reports;
- Department and local policies and procedures pertaining to the Incidents of Security Concern Program;
- Department and local cyber security policies and procedures; and
- Prior OIG reports.

Also, pursuant to the Government Performance and Results Act of 1993, we determined that Y-12 had established performance measures related to cyber security at the site.

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 OIG reports:

- “Internal Controls Over Computer Property at the Department’s Counterintelligence Directorate” (DOE/IG-0762, March 2007);
- Special Inquiry on “Selected Controls over Classified Information at the Los Alamos National Laboratory” (OAS-SR-07-01, November 2006);
- “Department of Energy’s Fiscal Year 2006 Consolidated Balance Sheet” (OAS-FS-07-02, November 2006);
- “Management Controls over the Federal Energy Regulatory Commission’s Unclassified Cyber Security Program – 2006” (OAS-M-06-10, September 2006); and,
- “The Department’s Unclassified Cyber Security Program – 2006” (DOE/IG-0738, September 2006).

# Appendix C


---



Department of Energy  
National Nuclear Security Administration  
Washington, DC 20585  
November 13, 2007



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 Y-12 Security Incident;  
S07IS011; IDRMS No. 2007-04290

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, "Incident of Security concern at the Y-12 National Security Complex." We understand that this inspection was conducted because the IG received an allegation that electronic devices were inappropriately taken into a Y-12 Limited Area and you wanted to determine the facts and circumstances surrounding the allegation.

We believe that the report as written should be categorized as Official Use Only. We have documentation that supports this position or the Site Office can provide the same documentation.

I am submitting the following comments for accuracy or to make it more clear to the reader:

- Page 1, Second Paragraph, Second Sentence - Delete the reference to "special nuclear material." Since this incident did not involve special nuclear material, the reference should be deleted to avoid any misinterpretation.
- Page 1, Second Paragraph, Fifth Sentence - We recommend that this sentence read for accuracy: "Such capabilities are restricted or prohibited, without proper approvals, in secure environments in order to protect against the disclosure of sensitive classified information by the user or monitoring or intrusion by external threats."
- Page 2, First Bullet, Second Sentence - This sentence should read for accuracy: "Per DOE orders, since status reports are not required for Impact Measurement Index (IMI) 3 incidents, the next report required to identify the total number of laptops associated with the incident was the final investigative report which was submitted to headquarters in May 2007 as required."
- Page 6, Paragraph 1, First Sentence - This sentence should read for accuracy: "connectivity had been made; and if any of the computers contained "malware" (a general term coined for a variety of malicious and non-malicious software)."





## Appendix C (continued)

---

2

- Third Sentence - Should read for accuracy: "The CFL explained that while malware can have legitimate applications and is commonly found on most computers, some types have the potential to cause harmful, destructive or intrusive actions and can be used to capture a user's keystrokes to provide a means of obtaining unauthorized information. It is noted there is no evidence that any software attempted to exploit the Y-12 network or otherwise cause any cyber security breach."
- Page 6, Paragraph 2, Second Sentence - Sentence should read for accuracy: "Following the completion of Y-12 mandated training, BWXT Y-12 reviewed ORNL reinstatement requests, and reinstated facility access only for those ORNL employees deemed appropriate."

In discussions with the Site Office, we believe that the recommendations, not only are appropriate, but that all actions related to the recommendations have been completed (NNSA did not address recommendations 1 and 2 in the report since they are addressed to the Manager, Oak Ridge).

- Policies/procedures have been reviewed and updated to include requirements related to laptop computers. Equipment seizure processes have been defined and reporting requirements for incidents affecting multiple sites have been updated
- Oak Ridge personnel have been retrained prior to being granted reaccess to Y-12. Network Monitoring Procedure was updated and the Site's cyber first responders have been trained/retrained.
- We continue to conduct frequent reviews and conduct random inspections related to compliance in cyber security disciplines.
- We have reemphasized timely reporting requirements and are updating local procedures.
- We have conducted an extensive review of procedures related to the sharing of information with counterintelligence officials and have edited our procedures accordingly.

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

cc: Ted Sherry, Manager, Y-12 Site Office  
Bill Desmond, Chief, Defense Nuclear Security  
Cheryl Stone, Acting Associate Administrator for Defense Nuclear Security  
Karen Boardman, Director, Service Center

# Appendix C (continued)

---

DOE F 1325.6  
(3/96)

~~OFFICIAL USE ONLY~~

United States Government

Department of Energy

Oak Ridge Office

## memorandum

DATE: November 2, 2007

REPLY TO:  
ATTN OF: FM-733:Miller

SUBJECT: **DRAFT INSPECTION REPORT ON "INCIDENT OF SECURITY CONCERN AT THE Y-12 NATIONAL SECURITY COMPLEX" (SO71S011)**

TO: Christopher R. Sharpley, Deputy Inspector General for Investigations and Inspections,  
IG-1, FORS

This is in response to your October 15, 2007, memorandum with attached draft report, subject as above. The following information is the Management Response to the recommendations noted in the subject report. The Oak Ridge Office (ORO) concurs with the recommendations, and we have included the corrective actions that were initiated and have been completed since the onset of this inspection.

### Recommendation No. 1:

**Hold accountable those individuals who violated Department and site policies and procedures.**

### Management Response:

Concur. Immediately upon notification, the Department of Energy (DOE) ORO, National Nuclear Security Administration/Y-12 Security Organization, Y-12, and the Oak Ridge National Laboratory (ORNL) senior management initiated a series of rapid precautionary and corrective actions due to this incident. The corrective actions have all been completed.

The corrective actions for the proper control and custodianship of the computers and access to the facility taken included: immediate suspension of Y-12 user IDs for the ORNL; computer administration and security duties for some personnel were removed from and reassigned to other ORNL staff; all 38 laptops were turned in, evaluated, and

Document/Material Transmitted  
Contains Official Use Only  
Information. When separated from  
attachment, this document **does not**  
contain Official Use Only  
Information.

~~OFFICIAL USE ONLY~~

## Appendix C (continued)

---

~~OFFICIAL USE ONLY~~

Christopher R. Sharpley

-2-

November 2, 2007

reviewed by DOE's Cyber Forensic Laboratory, federal law enforcement offices, and other cyber security; relocation of ORNL staff to offices on the ORNL main campus; ORNL internal procedures on use of laptops were re-emphasized to all ORNL staff; and additional actions that further strengthened and enhanced the work control procedures.

**Recommendation No. 2:**

**Conduct refresher training of all employees to ensure they understand the applicable requirements and their individual responsibilities with respect to the issues raised in this report.**

**Management Response:**

Concur. Since the time of the fieldwork for this review, a number of immediate actions occurred such as comprehensive security training with emphasis on computer security and Cyber Security in Limited Areas. In addition, the ORNL Director has held two sessions with approximately 500 cleared personnel to address the importance of security to the overall ORNL mission and re-emphasize the ORNL commitment to security. By February 2008, the annual Security Refresher training required for all cleared personnel will be completed.

In addition, I have also included as attachments, the general comments that are our suggested revisions to the report and a detailed listing of the corrective actions taken. The attachments are Official Use Only.

We request that your staff return to the site to verify completion of the corrective actions before the final report is issued. If there are any questions or additional information is required, please contact me at 865-576-4446 or Johnny Moore at 865-576-3536.

  
Judith M. Penry  
Chief Financial Officer

**Attachments:**

1. General Comments to Draft Report
2. Corrective Actions in Response to Recommendations

**cc w/attachments:**

G. J. Malosh, SC-3, FORS  
G. G. Boyd, M-1, ORO  
R. J. Brown, M-2, ORO  
J. O. Moore, SC-10, ORO

~~OFFICIAL USE ONLY~~

## 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 more clear 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.