



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

# Inspection Report

## Internal Controls over Computer Hard Drives at the Oak Ridge National Laboratory

INS-O-10-03

August 2010



**Department of Energy**  
Washington, DC 20585

August 16, 2010

MEMORANDUM FOR THE DIRECTOR, OFFICE OF SCIENCE

*Sandra D. Bruce*

FROM: Sandra D. Bruce  
Assistant Inspector General for Inspections and Special Inquiries

SUBJECT: INFORMATION: Inspection Report on “Internal Controls over  
Computer Hard Drives at the Oak Ridge National Laboratory”

BACKGROUND

The Department of Energy’s (Department) Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee, provides unique expertise in support of the Department’s science and national security portfolios. UT-Battelle, LLC, manages ORNL for the Department through the Oak Ridge Office. ORNL’s mission frequently involves producing and receiving sensitive electronic information, data which requires special handling to protect against unauthorized disclosure. Of its approximately 16,400 computers, over 6,200 produce, store or transfer sensitive unclassified information, such as Official Use Only and Personally Identifiable Information (PII) (e.g. name, social security number and medical history). Department guidance requires that storage media no longer in use, but previously used to process sensitive unclassified information, be either protected by approved encryption or tracked and controlled until purged or destroyed. After receiving an allegation that computer hard drives were being removed by unauthorized individuals, a practice that could potentially result in the unauthorized release of sensitive unclassified information, the Office of Inspector General initiated an inspection to review the facts and circumstances of the allegation.

RESULTS OF INSPECTION

We concluded that ORNL did not have adequate internal controls to effectively track and control hard drives which potentially contain sensitive unclassified information. Specifically, ORNL had not implemented controls to encrypt, or track and control, hard drives that may contain sensitive unclassified information. Division Computer Security Officers (DCSOs), who are responsible for identifying and addressing computer security concerns, informed us that they recovered hard drives from unsecure locations, such as unoccupied offices, hallways, and docks. Also, after recovering these hard drives, the DCSOs told us that they could not give us an accurate count of the number of hard drives in their possession. To clarify the scope of this potential vulnerability, we requested that ORNL conduct a survey to account for the total number of hard drives secured by the DCSOs. In response to our request, ORNL identified approximately 1,500 hard drives that were secured and stored by ORNL DCSOs at the site. In reviewing the survey results, we noted significant disparity between the number of hard drives

estimated by the DCSOs and the actual number recovered. Although the DCSOs controlled and stored the hard drives, they acknowledged that the hard drives had not been formally tracked, as required.

We also reviewed ORNL's Campus Support and Instrumentation Division's hard drive database. The Division's instrument technicians are responsible for removing hard drives from excessed computers. A review of the database revealed that hard drives were missing from 424 computers of which 193 had been used to process information in sensitive program areas, such as the Health Services Division and those located in the Limited Security Area. In accordance with ORNL policies, fixed (non-removable) computer hard drives are only to be removed from excessed computers by Campus Support technicians. Nothing came to our attention to suggest that there had been a compromise of system information. However, the concerns raised during the inspection suggest that ORNL was not making the maximum use of readily available measures to prevent compromise.

To address these matters, we made recommendations to the Manager, Oak Ridge Office.

#### MANAGEMENT REACTION

In comments on a draft of this report, Oak Ridge Office officials concurred with the report recommendations, but took exception to some of our analysis regarding the requirement to track or encrypt hard drives; the finding of hard drives in unoccupied rooms; and, the unauthorized removal of hard drives. We addressed management's concerns in the report.

#### Attachment

cc: Deputy Secretary  
Under Secretary for Science  
Chief of Staff  
Director, Office of Risk Management, CF-80  
Manager, Oak Ridge Office  
Team Leader, Office of Risk Management, CF-80  
Audit Resolution Specialist, Office of Risk Management, CF-80

# REPORT ON INTERNAL CONTROLS OVER COMPUTER HARD DRIVES AT THE OAK RIDGE NATIONAL LABORATORY

---

## TABLE OF CONTENTS

### OVERVIEW

Introduction and Objective .....	1
Summary .....	1

### DETAILS OF FINDINGS

Inadequate Controls Over Hard Drives .....	4
Other Matters .....	8

<u>RECOMMENDATIONS</u> .....	8
------------------------------	---

<u>MANAGEMENT AND INSPECTOR COMMENTS</u> .....	9
--	---

### APPENDICES

A. Scope and Methodology .....	11
B. Prior Reports .....	12
C. Management Comments .....	13

### **INTRODUCTION AND OBJECTIVE**

The Department of Energy's (Department) Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee, provides technology and expertise in support of the Department's science and national security portfolios. UT-Battelle, LLC, manages ORNL for the Department through the Oak Ridge Office. ORNL's mission frequently involves producing and receiving sensitive electronic information data, which requires special handling to protect against unauthorized disclosure. Of its approximately 16,400 computers, over 6,200 produce, store or transfer information, including sensitive unclassified information, such as Official Use Only and Personally Identifiable Information (PII) (e.g. name, social security number and medical history). As part of its normal procedures, ORNL excesses approximately 2,000 computers annually, many of which may have processed sensitive unclassified information.

To help protect sensitive unclassified information, the Department has issued specific tracking, controlling, purging and destruction guidance. In addition to Department regulations, ORNL has issued internal guidance and cyber security requirements which focus on protecting such information from inappropriate release.

After receiving an allegation that computer hard drives were being removed by unauthorized individuals, a practice that could potentially result in the unauthorized release of sensitive unclassified information, the Office of Inspector General initiated an inspection. The inspection was initiated to determine whether:

- ORNL had adequate internal controls to track and control excessed computer hard drives;
- Internal computer hard drives at ORNL were being removed contrary to ORNL's cyber security policies and procedures; and,
- The circumstances surrounding the removal and disposal of hard drives at ORNL were consistent with requirements in place at the time of our review.

### **SUMMARY**

We concluded that ORNL's controls over the tracking of hard drives, which may contain sensitive unclassified information, were inadequate to prevent the unauthorized dissemination of sensitive unclassified information. Specifically, ORNL had not implemented controls to encrypt or track and control hard drives. Department guidance requires that storage media no longer in use,

---

but previously used to process sensitive unclassified information, be either protected by approved encryption or tracked and controlled until purged or destroyed.

During our review, Division Computer Security Officers (DCSOs), who are responsible for identifying and addressing computer security concerns, informed us that hard drives were removed from computers without authorization, and had been abandoned in unoccupied offices, hallways, and other locations. This was an apparent disregard for established procedures. These hard drives were subsequently collected and secured by the DCSOs. We requested that ORNL conduct a survey to determine the number of hard drives stored and secured by the DCSOs.<sup>1</sup> As a result of our request, ORNL identified approximately 1,500 hard drives (which were no longer in use) that were secured and stored by the DCSOs at the site.

In January 2007, the Department issued Cyber Security Program Chief Information Officer Guidance CS-11, “Media Clearing, Purging, and Destruction Guidance,” which notes that storage media no longer in use, which was previously used to process sensitive unclassified information, must be tracked and controlled until purged or destroyed.<sup>2</sup> These protective measures for sensitive unclassified information are intended to minimize the potential of the inadvertent disclosure of information while increasing the difficulty of unlawfully obtaining such information.

We noted that ORNL policy requires full disc encryption for all laptop computers. However, for desktop computers, ORNL had not implemented existing Department guidance to encrypt or track and control hard drives associated with sensitive unclassified systems. ORNL internal policy prohibits individuals other than Campus Support and Instrumentation Division instrument technicians (Campus Support technicians) from removing hard drives from computers. However, our review of the Campus Support technicians’ database revealed that hard drives were removed by someone other than the authorized technicians. Specifically, hard drives were missing from 424 computers (11 were laptop computers) of which 193 had been used to process

---

<sup>1</sup> The total number of hard drives stored and secured included abandoned hard drives and hard drives turned in to the DCSOs. The survey would be beneficial in determining the accountability of hard drives which may contain sensitive unclassified data.

<sup>2</sup> CS-11 has been replaced by the Department’s issued Cyber Security Technical and Management Requirements, “Media Clearing, Purging, and Destruction (TMR-10)”.

---

information in sensitive program areas, such as the Health Services Division and those located in the Limited Security Area (LSA). While we are not aware of any resulting compromise, these types of weaknesses expose the Department to the risk that sensitive mission and PII information may be compromised. We coordinated with Oak Ridge Office and ORNL officials during our fieldwork. In response to our findings, ORNL officials initiated a number of corrective actions to track hard drives used to process such information. These actions included:

- Notifying ORNL employees of ORNL's policy that fixed (non-removable) computer hard drives are only to be removed from excess computers by Campus Support technicians. ORNL is currently working on addressing employee awareness and also anticipates revising its cyber security training on this topic;
- Removing and destroying approximately 1,500 hard drives; and,
- Taking action to implement the Department's most current guidance and requirements on tracking hard drives used in processing sensitive unclassified information.

The Office of Inspector General has completed several reviews related to information security, expressing concerns regarding the ability of Department sites to protect sensitive unclassified information. An August 2009 OIG report identified the concern that various Department sites were not encrypting sensitive information contained on desktops. A list of the associated reports is found at Appendix B.

## Details of Findings

---

### **INADEQUATE CONTROLS OVER HARD DRIVES**

We concluded that ORNL did not have adequate internal controls to effectively encrypt or track and control hard drives that potentially contain sensitive unclassified information. Computer Support technicians and DCSO informed us that hard drives were removed from computers by unauthorized personnel and, in some instances, abandoned in various locations. This situation occurred because some ORNL employees were not aware of the requirement that only technicians were authorized to remove hard drives; and ORNL had not implemented effective control measures. In this regard, officials had not ensured that responsible employees complied with ORNL internal guidelines or the Department's guidance and requirement to encrypt or track and control, hard drives containing sensitive unclassified information. This situation increased the potential for the compromise of sensitive unclassified information.

### **Recovered Hard Drives**

The DCSOs informed us that numerous hard drives had been recovered from unoccupied ORNL offices, hallways, docks and other locations. These hard drives, some from computers used in sensitive areas, were removed without authorization, abandoned in various locations and subsequently found by DCSOs and secured. The identity of the individuals abandoning those hard drives was unknown to the DCSOs. Although the DCSOs subsequently controlled and stored the hard drives, none of the DCSOs provided evidence that the hard drives were formally tracked. To emphasize this lack of tracking, one DCSO we interviewed estimated approximately 100 recovered hard drives were in storage, but when he took us to an adjacent building, we counted only 55 recovered hard drives. These hard drives have been stored in two locked rooms for years since being secured from various offices and laboratories.

In order to determine the number of untracked hard drives residing with the DCSOs, we requested that Laboratory officials conduct a survey to identify hard drives secured and stored by ORNL which were no longer in use. As a result of our request, the DCSOs identified approximately 1,500 hard drives, including the 55 originally identified in our review. After conducting this assessment, ORNL management took immediate action and destroyed the 1,500 hard drives in accordance with Department regulations.

The survey results also identified 66 recovered hard drives that were identified and collected by the DCSO we mentioned previously. No explanation was ever provided to account for the additional 11 hard drives. In fact, the survey identified several



---

other DCSOs with a significant disparity between the estimated number of hard drives in storage and those actually recovered, the largest discrepancy of which was 159 fewer hard drives collected than was originally estimated by the DCSO. The lack of controls identified in our report and the disparity noted above raised additional concerns regarding the potential for compromised information.



Hard drive storage

During interviews, several DCSOs acknowledged that certain of the hard drives contained PII or opined the likelihood of such. To determine whether any of the hard drives contained PII, we requested that the Office of Inspector General's Office of Investigations conduct a forensic examination of a hard drive that another DCSO indicated was found unsecured. In this case, the owner was never known to the DCSO. The forensic examination of the hard drive revealed that the hard drive contained sensitive unclassified information. Specifically, the examination of the hard drive revealed 21 pages of PII, including the name, date of birth, and medical information pertaining to an ORNL employee.<sup>3</sup> The hard drive also contained the individual's salary/deduction wage allocations, which ORNL treats as sensitive unclassified information, and assorted scientific research data.

The inspection did not determine whether the personal information was generated by the individual on his or her work computer for personal use or by ORNL's Health Services Division, Human Resources Directorate, or otherwise maintained by UT-Battelle or

---

<sup>3</sup> In accordance with Department policy, we notified the Office of Cyber Security regarding this issue.

---

the Department. In accordance with the Department's Chief Information Officer Guidance CS-38A, "Protection of Sensitive Unclassified Information, Including Personally Identifiable Information," UT-Battelle does not consider personal information stored by individuals about themselves on their assigned workstations or laptops at ORNL to be PII. Therefore, such information is not subject to Department protection requirements for sensitive unclassified information, unless it contains a social security number. ORNL's policy, "Requirements for Protected Personally Identifiable Information," defines PII as "An individual's first name or first initial and last name in combination with any one or more of the following types of information including, but not limited to, medical, and financial records, etc."

Senior ORNL officials indicated that "encryption and tracking are not currently required by the ORNL contract." The officials further stated that ORNL is in compliance with the current Office of Science's Program Cyber Security Plan (PCSP), which has not been updated since 2007. However, the Department requires that Departmental elements, including the Office of Science, which manages ORNL, develop cyber security requirements through a Program Cyber Security Plan (PCSP) using a risk-based approach. Specifically, the Office of Science's PCSP requirement is to implement Department Manual 205.1-2, "Clearing, Sanitization, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Manual." Senior ORNL officials stated that 205.1-2 does not require encryption or tracking of hard drives. However, we noted that Department Manual 205.1-6, "Media Sanitization Manual," issued in December 2008, requires that storage media no longer in use, previously used to process sensitive unclassified information, must either be protected by approved encryption or tracked and controlled until purged or destroyed.

According to a senior Headquarters official responsible for maintaining and developing the PCSP for the Office of Science, ORNL is required to implement Department Manual 205.1-2 with consideration of Departmental Guidance CS-11, "Media Clearing, Purging, and Destruction Guidance." CS-11, issued in January 2007, as a part of the Department's Cyber Security Revitalization Plan, identifies specific guidance concerning the tracking or control of storage media used to process sensitive unclassified information. The senior official stated that if ORNL officials did not implement CS-11, they should have documented that a risk assessment was conducted and formally identified the individual who assumed the risk to not implement the guidance. Oak Ridge

---

Office and ORNL officials were unable to provide documentation of the risk assessment conducted, nor could they provide the name or title of the individual accepting responsibility for not implementing Department guidance. The guidance noted in CS-11 is similar to the requirements in Department Manual 205.1-6, "Media Sanitization Manual," in that both require that sensitive information must be tracked and controlled until purged or destroyed. ORNL incorporated the requirements of Department Manual 205.1-6 in its contract in March 2009, but had not included the Manual requirements in its current ORNL Cyber Security Plan. A senior ORNL official from the Office of the Chief Information Officer informed us that, prior to our inspection there had been discussions of possibly encrypting hard drives for sensitive unclassified systems, or identifying systems that may contain such information and tracking the associated hard drives as part of ORNL's Cyber Security Plan. In September 2009, ORNL officials informed us that they had initiated actions to evaluate the implementation of tracking hard drives used to process sensitive unclassified information.

In a related Office of Inspector General report issued in August 2009, concerning the protection of sensitive unclassified information, we noted that sites reviewed were not encrypting sensitive information contained on desktops. Additionally, the National Institute of Standards and Technology (NIST) Special Publication 800-111, "Guide to Storage Encryption Technologies for End User Devices," had identified such an encryption practice as a "best practice" and part of an effective risk-based management approach to information protection.

## **Unauthorized Removal of Hard Drives**

We reviewed the hard drive database operated by the ORNL Campus Support technicians. Our review revealed that 424 hard drives were removed by someone other than the authorized technicians during the period of January 2008 to January 2009. Of the 424 hard drives, 193 were from sensitive program areas involved in national security, export control and medical information processing. The review also revealed that many computers had multiple hard drives installed, some up to 18. The removal of hard drives by unauthorized individuals as recognized by Department policy represents a vulnerability.

During our interviews, three property custodians and one DCSO acknowledged removing the hard drives for use as a storage device or for reuse in other computers. One DCSO informed us of instances in which computers waiting to be excessed were being taken by ORNL employees from unoccupied rooms or hallways.

---

In addition, 2 network administrators informed us that they had removed 10 hard drives from computers waiting to be excessed that were once used in sensitive program areas. This was done in order to reuse them in an internal networking device. When asked why they removed the hard drives, the administrators indicated they were unaware of ORNL's procedures which limits hard drive removal to Campus Support technicians. ORNL procedure entitled "Procedure for Disposition of Computers and Other Items with Media," specifies only ORNL's Campus Support technicians are authorized to remove internal hard drives.

Senior ORNL officials informed us that many of the hard drives were removed by non-Campus Support technicians prior to the issuance of its current policy. They further stated that hard drives for unclassified computers located in the Limited Security Area (LSA) must be removed prior to being excessed from the LSA, but the technicians were incorrectly completing the forms. The officials also indicated that improvements were made to the internal procedures, issued between January 2008 and December 2008, clarifying the Campus Support technicians' roles and responsibilities in hard drive disposition.

## **OTHER MATTERS**

Although outside the scope of our inspection, a DCSO informed us of computers being taken by some ORNL employees or disappearing while waiting to be excessed. During Fiscal Years 2007 and 2008, ORNL's Property Management Organization listed 11 computers stolen and 39 computers/servers lost (3 of those reported as lost were subsequently found). The computers were likely at the end of their useful life and were not of great value, but their disappearance and the lack of controls raised additional concerns regarding the potential for compromised information.

## **RECOMMENDATIONS**

Significant and timely corrective actions have been taken by ORNL to improve security controls for most of the vulnerabilities we identified; however, additional actions are warranted.

We recommend that the Manager, Oak Ridge Office:

1. Implement the Department's requirements concerning storage media no longer in use and previously used to process sensitive unclassified information, to protect the media by approved encryption, or tracking and control until purged or destroyed.
2. Ensure ORNL trains employees on its policy and procedures regarding removal of computer hard drives.

---

**MANAGEMENT AND  
INSPECTOR  
COMMENTS**

In comments on a draft of this report, the Department's Oak Ridge Office concurred with the recommendations. Although management concurred with our recommendation, they took exception to some of our analysis regarding the requirement to track or encrypt hard drives; the finding of hard drives in unoccupied rooms, and the unauthorized removal of hard drives.

Management's comments are included in their entirety in Appendix C of this report.

We consider management's comments and corrective actions planned and/or taken responsive to our recommendations. We have addressed management's comments below and made technical changes to the report, as appropriate.

Management said that the ORNL sanitization policies are in compliance with the current Office of Science (SC) Program Cyber Security Plan (PCSP). The PCSP states, "SC policy is to implement DOE M 205.1-2 with consideration of CS-11." Management observed that tracking or encryption of hard drives is not required. We acknowledge that DOE M 205.1-2 does not require tracking or encryption of hard drives; however, CS-11 does require storage media no longer in use, previously used to process sensitive unclassified information, be tracked and controlled until purged or destroyed. Furthermore, if ORNL officials considered but did not implement CS-11, they should have documented the risk assessment conducted and formally identified the individual who assumed the risk to not implement the guidance. The Oak Ridge Office and ORNL officials were unable to provide us that documentation.

Management commented that our reporting of hard drives found in unoccupied offices is misleading because offices used for storage were locked. While we agree that several unoccupied offices and locations used for storage were locked, we were told by DCSOs (who are responsible for accountability of hard drives) of instances in which hard drives were collected from unlocked offices and locations, which the DCSOs subsequently secured. Also, one DCSO informed us of instances in which computers awaiting excessing were being taken by ORNL employees from unoccupied rooms or hallways.

Management noted non-instrument technicians removed many hard drives prior to policy revisions and that some systems in the LSA had removable hard drives, accounting for some missing hard drives. Removable hard drives were not listed in our sample.

---

Also, we noted that the policy to restrict the removal of hard drives from unclassified systems, including systems in the LSAs, was implemented in October 2005. Consequently, it seems unlikely that hard drives removed from computers by non-technicians prior to October 2005 were part of our data sample. Also, management noted that several boxes of hard drives not associated with computers were turned in by ORNL personnel, indicating the awareness of needed sanitization. The collection of several boxes of hard drives not associated with computers raises additional concerns regarding the lack of controls and the potential for compromised information from other media.

### SCOPE AND METHODOLOGY

Our review included computer excessing policies and procedures at the Oak Ridge National Laboratory and Department. The majority of our fieldwork was conducted from January through April 2010. Our research, analysis and fieldwork activities included:

- Interviews with approximately 48 property custodians, DCSOs, security officials associated with over 30 ORNL program areas;
- Review of Department and local policies and regulations pertaining to internally transferred and excessed computers;
- Assessment of documents, survey results, and electronic spreadsheets regarding computers excessed, unaccounted for hard drives, abandoned hard drives, and lost or stolen computers;
- Coordination with the Office of Inspector General's Technology Crimes Section to recover information stored on a recovered and secured hard drive; and,
- Review of prior Office of Inspector General and Government Accountability Office reports, and other related reports.

This inspection was conducted in accordance with the Council of the Inspectors General on Integrity and Efficiency, "*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:

- “The Federal Energy Regulatory Commission’s Unclassified Cyber Security Program – 2009” (DOE/IG-0830, October 2009);
- “The Department’s Unclassified Cyber Security Program – 2009” (DOE/IG-0828, October 2009);
- “Protection of the Department of Energy’s Unclassified Sensitive Electronic Information” (DOE/IG-0818, August 2009);
- “Security Weaknesses in the Handling of Unclassified Printers and Copiers at the Oak Ridge National Laboratory” (INS-L-09-06, S08IS001, May 2009);
- “Personal Property Management at Lawrence Livermore National Laboratory” (INS-O-09-03, May 2009);
- Special Report: “Management Challenges at the Department of Energy” (DOE/IG-0782, December 2007);
- “Security Over Personally Identifiable Information” (DOE/IG-0771, July 2007);
- “Internal Controls Over Computer Property at the Department’s Counterintelligence Directorate” (DOE/IG-0762, March 2007); and,
- “Excessing of Computers Used for Unclassified Controlled Information at Lawrence Livermore National Laboratory” (DOE/IG-0759, March 2007).



DOE F 1325.8  
(302)

United States Government

Department of Energy  
Oak Ridge Office

# memorandum

DATE: May 12, 2010

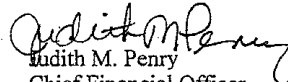
REPLY TO  
ATTN: FM-733:Pooler

SUBJECT: **DRAFT INSPECTION REPORT ON "INTERNAL CONTROLS OVER COMPUTER HARD DRIVES AT THE OAK RIDGE NATIONAL LABORATORY" (S09IS005)**

TO: Sandra D. Bruce, Assistant Inspector General for Inspections and Special Inquiries, Office of Inspections and Special Inquires, IG-40, FORS

In response to your memorandum dated April 21, 2010, transmitting the subject Draft Inspection Report, the Oak Ridge Office concurs with the recommendations as presented. Our comments on the accuracy of facts as well as our corrective actions planned and/or taken are provided in the attached.

If you have any questions or need additional information, please contact Tina Pooler of my staff at (865) 576-2654.

  
Judith M. Penry  
Chief Financial Officer

Attachment

cc w/attachment:  
Merley L. Lewis, CF-1.2, FORS  
Gerald G. Boyd, M-1, ORO  
Robert J. Brown, M-2, ORO  
Richard A. Dotson, AD-41, ORO  
Johnny O. Moore, SC-10, ORO  
Mark A. Million, SC-10, ORO

**OAK RIDGE OFFICE COMMENTS**  
**Office of Inspector General Draft Report, "Internal Controls Over Computer Hard Drives**  
**at the Oak Ridge National Laboratory" (S09IS005)**

**General Comments:**

1. **Page 1, 1<sup>st</sup> paragraph** – References to Unclassified Controlled Nuclear Information (UCNI) should be removed from this report; there is no need to mention UCNI when no UCNI information was or is believed to be compromised.
2. **Page 1, 1<sup>st</sup> paragraph, 4<sup>th</sup> sentence** – 16,440 computers are referenced here, but only 6,284 are currently registered in the ORNL Network Registration System as containing sensitive information, and 1,087 or about 18% of those are laptops. ORNL requires all laptops to have full disk encryption. There is a much smaller threat than implied.
3. **Page 1, 3<sup>rd</sup> paragraph, 1<sup>st</sup> sentence** – Suggest revising to: "After receiving an allegation that computer hard drives were being removed from computers by personnel other than described in ORNL procedures, which could potentially result in the unauthorized release of sensitive unclassified information, the Office of Inspector General initiated an inspection."
4. **Page 2, 2<sup>nd</sup> paragraph** – The ORNL sanitization policies are in compliance with the current Office of Science (SC) Program Cyber Security Plan (PCSP). The PCSP states, "SC policy is to implement DOE M 205.1-2 with consideration of CS-11". DOE M 205.1-2 does not mention tracking or encryption of hard drives as a requirement.
5. **Page 2, 1<sup>st</sup> paragraph, 5<sup>th</sup> sentence** – The comment that the hard drives were found in unoccupied offices is misleading. Many times unoccupied offices are used for storage. Several of these offices and locations were locked. Hard drives which were stored in locked areas are under positive control, and while several of them should probably have been excessed, they were not in public locations where they could have been taken and moved offsite.
6. **Page 2, 3<sup>rd</sup> paragraph, 3<sup>rd</sup> sentence** – "Our review revealed that hard drives were missing from 424 computers...". Many of these drives were removed by non-instrument technicians prior to revisions to policies and awareness training. In addition, it is also ORNL's policy for hard drives for unclassified computers located in Limited Security Areas (LSAs) be removed prior to the computer being excessed from the LSA. These systems and drives were handled appropriately with the possible exception that it may not have been instrument technicians removing the drives. This has been corrected. Some systems located in the LSAs had removable drives which also accounts for some of the computers missing hard drives. Finally, it should be noted that ORNL processed several boxes of drives that were not associated with computers but were turned in by ORNL personnel which indicates personnel were aware that drives needed to be sanitized. These 424 computers had or were in the process of being excessed by ORNL Property.

7. **Page 2, 3<sup>rd</sup> paragraph, 3<sup>rd</sup> sentence** – "...hard drives were missing from 424 computers (11 were laptop computers) of which 193 had been used to process data in sensitive program areas." Suggest revising to: "...hard drives were missing from 424 computers located at ORNL Property Sales for the purpose of excessing; 193 of these were from sensitive program areas where ORNL's policy is to remove the drives from the computers before leaving the area (LSAs). It is recognized by ORNL that many of these systems may have had removable hard drives due to their location or level of information processed. Any systems with removable hard drives would not require instrument technicians to remove these drives. ORNL learned that in some cases these drives were removed by instrument technicians who were not aware they were to indicate the removal of the drives by labeling and inputting information drives."
8. **Page 4, 1<sup>st</sup> paragraph, 3<sup>rd</sup> sentence** – suggest changing "hard drives were removed by unauthorized personnel" to "hard drives were removed from computers by unauthorized personnel." The original text could mislead the reader to believe that hard drives were removed from the facility when in fact it can only be stated with accuracy that hard drives were removed from computers.
9. **Page 4, 3<sup>rd</sup> paragraph** – The disparity between the estimated number and the actual number of hard drives is irrelevant.
10. **Page 6, 1<sup>st</sup> paragraph (at top of page), 2<sup>nd</sup> sentence** – The report includes a statement that "...personal information stored by individuals about themselves on their assigned workstation or laptop is not considered PII...". This statement is attributed to a senior ORNL official. This information is not attributed to a UT-Battelle official, but is contained in the Department's Chief Information Officer (CIO) Guidance CS-38A, "Protection of Sensitive Unclassified Information, Including Personally Identifiable Information." CS-38A clearly states that such personal information is not considered PII, and UT-Battelle continues to believe that it is appropriate and essential to include the requested reference to CS-38A. The report should make clear that the above statement is not based on a policy decision made by UT-Battelle management, but rather an application of explicit guidance from the Department CIO. By its terms, CS-38A applies to DOE contractors "that use and operate Government-furnished information technology systems for or on behalf of the DOE or host DOE information on their non-Government information technology systems." Therefore, it is appropriate for UT-Battelle to rely on this guidance in establishing policies for the protection of PII at ORNL.  
**Recommend changing report to:** The inspection did not determine whether the personal information was generated by the individual on his or her work computer for personal use or by ORNL Health Services Division, Human Resources Directorate, or otherwise maintained by another UT-Battelle or the Department. A senior ORNL official indicated that in accordance with the Department's Chief Information Officer Guidance CS-38A, *Protection of Sensitive Unclassified Information, Including Personally Identifiable Information*, UT-Battelle does not consider "personal information stored by individuals about themselves on their assigned workstation or laptop" at ORNL is not considered to be PII and, therefore, such information is not subjected to Department protection requirements for sensitive unclassified information, "unless the information also it contains the individual's a social security number."

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

1. **“Implement the Department’s requirements concerning storage media no longer in use and previously used to process sensitive unclassified data, to protect the media by approved encryption, or tracking and control until purged or destroyed.”**

**Concur.** In accordance with Contract Document Requirement (CRD) of the DOE M 205.1-6, *Media Sanitization Manual*, which UT-Battelle accepted in the contract in December 2009, and is soon to be superseded by the DOE revised DOE Order (in RevCom), ORNL is required to implement a media sanitization process prescribed in the SC PCSP which is under major revision to include the requirement of DOE M 205.1-6 or new DOE Order related to media sanitization process. When SC releases the revised PCSP, ORO will direct ORNL to provide an implementation plan addressing tasks along with the funding requirement to implement the media sanitization process prescribed in the revised SC PCSP.

2. **“Ensure ORNL trains employees on its policy and procedures regarding removal of computer hard drives.”**

**Concur.** The ORNL Six Sigma Team assigned to address the disposition and disposal of hard drives was formed prior to the issuance of the draft report. The Team is currently working on a method to track hard drives when removed from computers, as well as addressing employee awareness. Awareness bulletins have already been issued, and the plan is to continue this on a routine basis. Completion date is September 30, 2010.

## 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 Felicia Jones at (202) 586-7013.

This page intentionally left blank.

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.