



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

Inspection Report

Internal Controls Over Computer
Property at the Department's
Counterintelligence Directorate

DOE/IG-0762

March 2007



Department of Energy

Washington, DC 20585

March 28, 2007

MEMORANDUM FOR THE SECRETARY

FROM:

Greg Friedman
Gregory H. Friedman
Inspector General

SUBJECT:

INFORMATION: Inspection Report on "Internal Controls Over Computer Property at the Department of Energy's Counterintelligence Directorate"

BACKGROUND

The Department of Energy's Counterintelligence Directorate, which is part of the Office of Intelligence and Counterintelligence, is responsible for protecting Departmental sensitive data and operations against espionage or other intelligence activities by foreign entities. In support of its mission, Counterintelligence maintained an extensive inventory of computer processing equipment. The objective of this inspection was to evaluate the adequacy of internal controls over computers and related property entrusted to the Counterintelligence Directorate's Headquarters program office.

RESULTS OF INSPECTION

Despite expending significant effort, the Counterintelligence Directorate was unable to locate 20 desktop computers which were part of its documented property inventory. While any loss of a computer is troubling, this situation was compounded by the fact that at least 14 of the computers were known to have processed classified information. The remaining six computers may have been used to process such data. Further, the inventory records were so imprecise and inaccurate that the Directorate had to resort to extraordinary means to locate an additional 125 computers. Those computers should have been readily accessible, had property record keeping been current and complete. Based on these findings, we concluded that Counterintelligence was unable to assure that the computers for which it is accountable, and, the often highly sensitive and/or classified information they processed, were appropriately controlled or were adequately safeguarded from loss and theft.

In addition, we found that:

1. Fifty-seven computers were not included on the Counterintelligence Directorate's property inventory, as required by the Department's Property Management Standards;
2. The Counterintelligence Directorate had expired loan agreements for 96 Headquarters computers that were located at its field sites; and,



Printed with soy ink on recycled paper

3. Labels indicating the classification level of individual computers were not affixed to 74 of the Counterintelligence Directorate's computers, as required.

Problems with the control and accountability of desktop and laptop computers have plagued the Department for a number of years. As we found in several recent reviews, strict property management procedures need to be consistently applied to ensure the control of sensitive property, such as computers. Moreover, a robust program of review and evaluation needs to be in place to assure that all computers and computer-related resources are accounted for and controlled. It was apparent that the Counterintelligence Directorate did not have procedures and processes in place to achieve this objective.

The report included a series of recommendations to address and resolve these issues. We recommended, as well, that, consistent with Department policy, management report to the Office of Security Operations all the computer property items that had not been located. The primary purpose of this notification is to initiate an inquiry to determine if the computers were lost or stolen and to ensure appropriate follow-up activities. The Counterintelligence Directorate believed, but could not confirm, that the computers had been accessed at some point in time. The Directorate did not report these items to Security Operations as lost or stolen until after we conducted our inspection.

MANAGEMENT REACTION

Management agreed with our recommendations. However, because the comments did not include planned corrective actions with target completion dates, a Management Decision is required. Management's comments are provided in their entirety in Appendix B of the report.

Attachment

cc: Deputy Secretary
Acting Under Secretary of Energy
Under Secretary for Science
Acting Administrator, National Nuclear Security Administration
Chief of Staff
Director, Office of Intelligence and Counterintelligence
Director, Office of Management
Chief Health, Safety and Security Officer
Director, Office of Internal Review (CF-1.2)
Director, Policy and Internal Controls Management (NA-66)

INTERNAL CONTROLS OVER COMPUTER PROPERTY AT THE DEPARTMENT'S COUNTERINTELLIGENCE DIRECTORATE

TABLE OF CONTENTS

OVERVIEW

Introduction and Objective	1
Observations and Conclusions	2

DETAILS OF FINDINGS

Property Not Located	3
Property Not in Inventory	4
Expired Loan Documentation	5
Computers Not Properly Labeled	5

<u>RECOMMENDATIONS</u>	5
-------------------------------------	---

<u>MANAGEMENT COMMENTS</u>	6
---	---

<u>INSPECTOR COMMENTS</u>	6
--	---

APPENDICES

A. Scope and Methodology	7
B. Prior Sensitive Property Reports	8
C. Management Comments	9

Overview

INTRODUCTION AND OBJECTIVE

The Office of Intelligence and Counterintelligence conducts technical analyses of foreign intelligence for the Department of Energy (DOE), including the National Nuclear Security Administration, and the United States Intelligence Community. The Counterintelligence Directorate (CN), which is part of the Office of Intelligence and Counterintelligence, is responsible for protecting DOE information against espionage or other intelligence activities by foreign entities. In support of this mission, CN procures and maintains computer processing equipment such as desktop computers, laptop computers, and computer servers. DOE considers computer property to be “sensitive property,” which is required to have specific controls in place. The objective of this inspection was to determine the adequacy of internal controls over computer property maintained by the CN Headquarters program office.

The Office of Inspector General (OIG) has issued several reports relating to accountability and internal controls over sensitive property. These reports are listed in Appendix B. In March 2006, we issued a report entitled “Internal Controls Over Sensitive Property in the Office of Intelligence,” DOE/IG-0722. Officials with the Office of Intelligence informed us that they had improved their property accountability system subsequent to our review. At the time of that review, the Office of Intelligence was separate from what was then called the Office of Counterintelligence. In March 2006, the two offices were consolidated into the Office of Intelligence and Counterintelligence. We have been informed that CN’s sensitive property will be consolidated into the Office of Intelligence and Counterintelligence’s property accountability system in the near future.

OBSERVATIONS AND CONCLUSIONS

Internal controls over classified and unclassified computer property at CN were inadequate. Specifically, CN could not locate 20 desktop computers listed on its property inventory that either processed or may have processed classified information. We identified control weaknesses that further undermined confidence in CN's ability to assure that its computers and the information they contain were appropriately controlled; were adequately safeguarded from loss and theft; and, were controlled in accordance with existing security requirements.

We further noted that:

- Fifty-seven computers were not included on CN's property inventory, as required by DOE's Property Management Standards;
- CN had expired loan agreements for 96 Headquarters computers that were located at CN field sites; and,
- Labels indicating the classification level of individual computers were not affixed to 74 CN computers, as required.

Concerns about the complex-wide system of computer controls and accountability have plagued the Department for a number of years. As we found in several recent OIG reviews, strict property procedures need to be consistently applied to classified and unclassified computers and a robust program of review and evaluation needs to be in place to assure that all computer resources are accounted for and controlled. It was apparent that CN did not have procedures in place to achieve this objective. Considering the sensitivity of the data regularly processed in CN, the shortcomings identified during our review were of major concern.

Details of Findings

PROPERTY NOT LOCATED

We found that CN could not locate 20 desktop computers listed on its property inventory that either processed or may have processed classified information.

During our initial inventory of 618 computers assigned to CN Headquarters, CN was unable to locate 241 computers. Subsequently, CN located all but 20 of these items. CN indicated that 14 of these 20 computers processed classified information at the Secret level and the remaining 6 could have processed classified information. CN concluded it could not find the 20 computers or find appropriate documents that addressed their ultimate disposition.

A “Retirement Work Order” (RWO) was used to remove lost, stolen, or damaged items from an office’s inventory. Following inquiries by the OIG, CN submitted RWOs for these 20 computers to the DOE Office of Management, which maintains the database of CN sensitive property at Headquarters. The RWOs for all 20 items indicated that CN believed that these items were excessed at some point in time. For example, there was evidence that at least 2 items were possibly excessed in 2002, although CN did not have confirmatory documentation regarding the disposition of these or any of the 20 computers.

We also noted an anomaly with the RWOs. CN listed one computer on a January 11, 2007, RWO as being excessed at a CN field location, despite the fact that the OIG located the computer in question at CN Headquarters in late December 2006. Once notified that the OIG had previously located this computer, CN conducted a search for the unit and located it in late January 2007. On January 30, 2007, CN informed the Office of Management it had “erroneously” listed this computer on the recent RWO document. We learned that the computer was placed back into CN’s inventory.

DOE Manual 470.4-1, “Safeguards and Security Program Planning and Management,” specifies that any suspected or confirmed loss of classified matter by any “medium, method, or action” be reported as a security incident. Additionally, the DOE Headquarters Personal Property and Supply Management Operating Procedures states that a program office’s Accountable Property Representative must report all stolen, lost or damaged property to the Office of Security Operations.

Not until after our inquiries did CN report 11 of these items to the DOE Office of Security Operations. Further, CN took the position

that the remaining nine computers did not need to be similarly reported because CN believed they were excessed by the field sites to which the computers had been loaned. An Office of Security official advised us that the circumstances represented by these nine items is a “gray area” in the reporting requirements and that it is at the discretion of the program office whether to report the items.

We noted that one of the computers reported to the Office of Security Operations as missing was the one that the OIG located in December 2006. As indicated above, this item was listed on an RWO and then later returned to the CN inventory. We also noted that although labeled as an unclassified computer when located by the OIG in December 2006, CN informed the Office of Security Operations that it had processed information at the Secret level.

We believe that because of the potential security implications and the fact that CN does not have definitive information as to the disposition of these items, it should report the circumstances regarding the remaining nine computers to the Office of Security Operations to determine whether an actual loss or theft had taken place.

**PROPERTY
NOT IN INVENTORY**

We found that 57 computers were not included on CN’s property inventory, as required by DOE’s Property Management Standards. DOE Property Management Standards, found in 41 Code of Federal Regulations Part 109, specifies that all sensitive property, including computer property, be controlled and inventoried annually.

During our initial inventory of CN computers, we physically identified 45 that were not in CN’s inventory. We determined that 14 of these 45 computers were from the Pacific Northwest National Laboratory (PNNL) and were sent to CN Headquarters at various times during the past four years. During our attempts to determine why the PNNL computers were not in CN’s inventory, we also learned that there were 12 additional PNNL computers that had been sent to CN Headquarters without having been entered into CN’s inventory. We determined that these computers had been transferred to another DOE program office during the past two years without proper transfer or accountability documentation. Additionally, we found paperwork that indicated another PNNL computer may have been sent to CN Headquarters. CN informed us that it had no evidence that the computer was ever received or utilized by CN Headquarters. We were unable to resolve this inconsistency.

EXPIRED LOAN DOCUMENTATION

We found that CN had expired loan agreements for 96 Headquarters computers that were located at CN field sites. We determined that 96 of the 241 items that we were unable to locate during our initial inventory were on loan to CN field sites. A loan agreement, which is to be generated by the organization transferring an item to another organization for a maximum of one year, had been prepared for the 96 computers as required. However, the loan agreements had expired in June and July 2006. Following inquiries from the OIG, CN generated new loan agreements for all but ten of these items. Regarding the remaining ten computers, CN disposed of eight of the computers and it advised us that new loan agreements are currently being prepared for the last two.

COMPUTERS NOT PROPERLY LABELED

We found that labels indicating the classification level of individual computers were not affixed to 74 CN computers, as required. Because CN maintains unclassified and classified computers in its offices, CN's Master Security Plan requires that all hardware be properly labeled as processing Unclassified, Confidential, or Secret information, as appropriate. Although not mentioned in the CN Master Security Plan, CN said that Top Secret computers also need to have labels.

RECOMMENDATIONS

Considering the sensitivity of the data regularly processed in CN and the shortcomings identified above, we recommend that the Director, Office of Intelligence and Counterintelligence ensure that:

1. Internal controls over Counterintelligence Directorate computer property are strengthened so that it is accounted for in a timely manner;
2. All items previously reported to the Office of Management on Retirement Work Orders are appropriately reported to the Office of Security Operations; and
3. All computer equipment assigned to the Counterintelligence Directorate is appropriately marked as processing Unclassified, Confidential, Secret, or Top Secret information.

**MANAGEMENT
COMMENTS**

In comments on our draft report, management agreed with the recommendations. Management's comments are included in their entirety at Appendix C.

**INSPECTOR
COMMENTS**

We found management's comments to be responsive to our recommendations. However, because the comments did not provide an implementation plan with target dates for each recommendation, a management decision is required.

Appendix A

SCOPE AND METHODOLOGY

This review included interviews with Federal and contractor officials with the DOE Office of Intelligence and Counterintelligence and the DOE Office of Management. We reviewed applicable policies and procedures pertaining to the management of computer property. We obtained CN's inventory listing from the Office of Management, which conducted an inventory of all CN property in 2006. We used this inventory listing as a baseline to conduct our inventory and evaluate CN's internal controls over computer property. We conducted a physical inventory of all CN computer property at Headquarters locations in Washington, DC, and Germantown, MD.

Also, pursuant to the "Government Performance and Results Act of 1993," we examined performance measurement processes as they related to computer property.

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

Appendix B

Prior Sensitive Property Reports

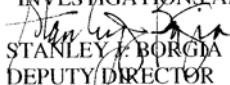
- “Excessing of Computers Used for Unclassified Controlled Information at the Idaho National Laboratory,” DOE/IG-0757, February 2007;
- “Destruction of Classified Hard Drives at Sandia National Laboratory-New Mexico,” DOE/IG-0735, August 2006;
- “Internal Controls for Excessing and Surplusing Unclassified Computers at Los Alamos National Laboratory,” DOE/IG-0734, July 2006;
- “Internal Controls Over Sensitive Property in the Office of Intelligence,” DOE/IG-0722, March 2006;
- “Control and Accountability of Emergency Communication Network Equipment,” DOE/IG-0663, September 2004;
- “Internal Controls Over the Accountability of Computers at Sandia National Laboratory, New Mexico,” DOE/IG-0660, August 2004;
- “Internal Controls Over Personal Computers at the Los Alamos National Laboratory,” DOE/IG-0656, August 2004;
- “Internal Controls Over Classified Computers and Classified Removable Media at the Lawrence Livermore National Laboratory,” DOE/IG-0628, December 2003;
- “Internal Controls Over Laptop and Desktop Computers at the Savannah River Site,” INS-L-03-09, July 2003;
- “Management of Sensitive Equipment at Selected Locations,” DOE/IG-0606, June 2003;
- “Inspection of Internal Controls Over Personal Computers at Los Alamos National Laboratory,” DOE/IG-0597, April 2003; and
- “Operations at Los Alamos National Laboratory,” DOE/IG-0584, January 2003.



Department of Energy
Washington, DC 20585

March 15, 2007

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

FROM: 
STANLEY J. BORGIA
DEPUTY DIRECTOR
COUNTERINTELLIGENCE DIRECTORATE
OFFICE OF INTELLIGENCE AND
COUNTERINTELLIGENCE

SUBJECT: Draft Report on "Internal Controls Over Computer Property
at the Department's Counterintelligence Directorate"
(S061S027)

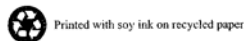
The Office of Intelligence and Counterintelligence has reviewed the draft report, *Internal Controls Over Computer Property at the Department's Counterintelligence Directorate* and agrees overall with the facts presented, the conclusions reached, and the recommendations addressed in the draft report.

The three recommendations listed in the report are: 1) that internal controls over Counterintelligence Directorate computer property are strengthened so that it is accounted for in a timely manner; 2) all items previously reported to the Office of Management on Retirement Work Orders are appropriately reported to the Office of Security Operations; and 3) all computer equipment assigned to the Counterintelligence Directorate is appropriately marked as processing Unclassified, Confidential, Secret or Top Secret information.

As a result of the Inspector General's March 2006 report, *Internal Controls Over Sensitive Property in the Office of Intelligence* (also referenced in the subject report), the now-merged Office of Intelligence and Counterintelligence instituted multiple measures to help strengthen its control of accountable property. These measures include the creation of a position for which the principal responsibility is property accountability, and the implementation of policies that require each piece of property be assigned to a specific user in a specific location and that requires the immediate report of the relocation of any accountable property item.

This Office would, however, like to address the following:

It is acknowledged that Retirement Work Orders (RWO) were submitted for 20 computers. However, since documentation exists, albeit not necessarily the proper documentation, that 9 of those 20 were excessed, or, turned in, by CN or Departmental



Appendix C

Field Sites, this Office believes those items should not be considered as missing and did not feel that a report to the Office of Security was necessary. The Office of Management requested that RWOs be submitted for those items so that they could be correctly removed from Department of Energy Headquarters' inventory, not because they were missing. This Office will, nonetheless, notify the Office of Health, Safety and Security regarding these items.

It should also be mentioned that 9 of the 11 computers that were RWO'd and subsequently submitted to security by this Office were legacy items that were procured and in some cases replaced before 2004, the year that CN implemented an automated tracking system for its computers systems and related equipment.

In closing, the Office of Intelligence and Counterintelligence would like to convey its appreciation for the professionalism of your Office during both computer property inspections over the past two years. We have found your inspectors to be fair and patient with our staff and very helpful in highlighting areas where our property accountability practices needed improvement.

cc: Rolf Mowatt-Larssen

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.

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.