



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

Inspection Report

Excessing of Computers Used for
Unclassified Controlled Information at
the Idaho National Laboratory



Department of Energy

Washington, DC 20585

February 16, 2007

MEMORANDUM FOR THE SECRETARY

FROM:

Greg Friedman
Gregory H. Friedman
Inspector General

SUBJECT:

INFORMATION: Inspection Report on "Excessing of Computers
Used for Unclassified Controlled Information at the Idaho National
Laboratory"

BACKGROUND

In support of its mission, the Department of Energy spends over \$2 billion each year on information technology and has a current inventory of approximately 800 information systems, including up to 115,000 personal computers, many powerful supercomputers, numerous servers, and a broad array of related peripheral equipment. The unclassified computers and electronic memory devices in these information technology systems often contain "unclassified controlled information." This term includes unclassified controlled nuclear information, proprietary information, export controlled information, official use only information, and personally identifiable information (PII), which can include employees' social security numbers, places of birth, and dates of birth.

When unclassified computers and other electronic memory devices are determined to be excess, they may be transferred for reuse within Department facilities or other governmental agencies, donated for educational purposes, sold, or salvaged. To prevent the unauthorized dissemination of unclassified controlled information, Department policy requires that, during the excessing process, data stored on computer hard drives and other memory devices must be properly removed or physically destroyed.

During an Office of Inspector General criminal investigation, it was determined that the Department's Idaho National Laboratory (INL) sold a computer containing unclassified controlled information, including PII, at a public auction in October 2004. Therefore, we initiated an inspection to evaluate the adequacy of INL's policies and internal controls for excessing computers and other electronic memory devices.

RESULTS OF INSPECTION

We concluded that INL did not have adequate policies and internal controls for excessing computers and other electronic memory devices to prevent the unauthorized dissemination of unclassified controlled information. Specifically, we found that INL did not always excess computers in accordance with applicable policies and procedures, which was clearly exemplified by its sale of the computer still containing unclassified controlled information. We did not,



however, identify any other unauthorized releases of unclassified controlled information. Our inspection also found that:

- INL's former management contractor did not revise and implement internal policies and procedures to reflect new requirements in a Department directive on clearing, sanitizing, and destroying information system storage media, memory devices, and other related hardware that was issued in February 2004. This may have been a contributing factor to the above mentioned improper release of a computer containing unclassified controlled information; and
- When a new company was awarded a contract in November 2004 to manage INL, the Department's Idaho Operations Office delayed incorporating Department directives on clearing, sanitizing, and destroying hard drives and memory devices into the contract. As a result, INL continued to follow existing internal policies and procedures and did not implement the requirements in the Department's directives for approximately 16 months.

In addition, while reviewing internal controls, we observed that:

- During the excessing process, INL could improve the physical safeguards provided for computers and other electronic memory devices that potentially contained unclassified controlled information.

The Department has experienced a number of problems in its efforts to appropriately excess computers and peripherals; control electronic memory devices; and, in general, administer its contracts. Many of these problems have been documented in prior reports issued by the Office of Inspector General. Based on our work in these areas, we have concluded that a key component to resolving these problems is the promulgation, implementation, and execution of effective policies and procedures. In that vein, to its credit, the Department took the important step of issuing complex-wide policy intended to specifically address the appropriate excessing of computers and the handling of electronic memory devices. However, at INL, as this report demonstrates, that effort was undermined when implementation of the Department's policy was delayed for over two years. Notably, 16 months of the delay occurred when Federal officials failed to incorporate the policy into the newly awarded INL site management contract. In our view, these delays were inconsistent with the Department's efforts to enhance the manner in which it administers its major contracts. Thus, we made several recommendations to management designed to enhance the security of sensitive information and to improve contract administration.

MANAGEMENT REACTION

In responding to a draft of this report, management concurred with our recommendations and identified corrective actions that have been or will be taken to address them. We found management's comments to be responsive to our findings and recommendations.

Attachment

cc: Deputy Secretary
Under Secretary of Energy
Under Secretary of Science
Administrator, National Nuclear Security Administration
Chief of Staff
Assistant Secretary for Nuclear Energy
Manager, Idaho Operations Office
Director, Office of Internal Review (CF-1.2)
Audit Liaison, Idaho Operations Office

EXCESSING OF COMPUTERS USED FOR UNCLASSIFIED CONTROLLED INFORMATION AT THE IDAHO NATIONAL LABORATORY

TABLE OF CONTENTS

OVERVIEW

Introduction and Objective	1
Observations and Conclusions	2

DETAILS OF FINDINGS

Release of Unclassified Controlled Information.....	3
INL Policies and Procedures.....	3
Delayed Policy Implementation.....	4
Safeguards for Hard Drives.....	5

<u>RECOMMENDATIONS</u>	7
-------------------------------------	---

<u>MANAGEMENT COMMENTS</u>	8
---	---

<u>INSPECTOR COMMENTS</u>	8
--	---

APPENDICES

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

Overview

INTRODUCTION AND OBJECTIVE

The Idaho National Laboratory (INL) is a Department of Energy (DOE) multi-program national laboratory that supports the mission of nuclear and energy research, science, and national defense. Battelle Energy Alliance, LLC (BEA), was awarded the contract to manage INL in November 2004 and assumed management responsibility for INL in February 2005. Prior to February 2005, Bechtel BWXT, LLC (BBWI) was the management contractor.

In support of research and other mission-related programs at its laboratories and facilities, DOE spends over \$2 billion each year on information technology and has a current inventory of approximately 800 information systems, including up to 115,000 personal computers, many powerful supercomputers, numerous servers, and a broad array of related peripheral equipment. The unclassified computers and electronic memory devices in these information technology systems often contain “unclassified controlled information.” This term includes unclassified controlled nuclear information, proprietary information, export controlled information, official use only information, and personally identifiable information (PII), which can include employees’ social security numbers, places of birth, and dates of birth.

DOE has long recognized the importance of protecting unclassified controlled information stored on computers and other electronic memory equipment, particularly when this equipment is no longer needed and becomes excess property. Excess property items, including unclassified computers, may be transferred for reuse within DOE facilities or other governmental agencies, donated for educational purposes, sold, or salvaged. To prevent the unauthorized dissemination of unclassified controlled information, DOE policy requires that, during the excessing process, data stored on computer hard drives and other memory devices must be properly removed or physically destroyed. Until recently, DOE approved methods for removing and/or destroying data on memory devices included: overwriting the data three times (often referred to as sanitizing); electronically destroying the data on the memory devices by using a degaussing machine; and physically pulverizing, incinerating, smelting, or disintegrating the memory devices. However, in September 2006, as a result of security concerns raised regarding degaussing, DOE’s Chief Information Officer issued guidance that degaussing should not be used as the sole means to purge data from hard disk drives or other magnetic computer storage media or devices.

During an Office of Inspector General criminal investigation, it was determined that INL sold a computer containing unclassified controlled information, including PII, at a public auction in October 2004. Therefore, we initiated an inspection to evaluate the adequacy of INL's policies and internal controls for excessing computers and other electronic memory devices.

OBSERVATIONS AND CONCLUSIONS

We concluded that INL did not have adequate policies and internal controls for excessing computers and other electronic memory devices to prevent the unauthorized dissemination of unclassified controlled information. Specifically, we found that INL did not always excess computers in accordance with applicable policies and procedures, which was clearly exemplified by its sale of the computer still containing unclassified controlled information. We did not, however, identify any other unauthorized releases of unclassified controlled information. Our inspection also found that:

- INL's former management contractor, BBWI, did not revise and implement internal policies and procedures to reflect new requirements in a DOE directive on clearing, sanitizing, and destroying information system storage media, memory devices, and other related hardware that was issued in February 2004. This may have been a contributing factor to the above mentioned improper release of a computer containing unclassified controlled information; and
- The DOE Idaho Operations Office delayed incorporating DOE directives on clearing, sanitizing, and destroying hard drives and memory devices into BEA's management contract. As a result, INL continued to follow existing internal policies and procedures and did not implement the requirements in the DOE directives for approximately 16 months.

In addition, while reviewing internal controls, we observed that:

- During the excessing process, INL could improve the physical safeguards provided for computers and other electronic memory devices that potentially contained unclassified controlled information.

Reviews by the Office of Inspector General at other DOE laboratories have also identified weaknesses in the excessing of computers and other electronic memory devices. A list of the associated reports is found in Appendix C.

Details of Findings

RELEASE OF UNCLASSIFIED CONTROLLED INFORMATION

We found that INL did not always excess computers in accordance with applicable policies and procedures, which was clearly exemplified by its sale of the computer still containing unclassified controlled information. At the time of the computer's sale in October 2004, INL was under BBWI management and was following an internal Management Control Procedure that had been in effect since October 2000. Under the Procedure, computers that met the requirements for reuse or donation to educational institutions were required to have the hard drives sanitized, and computers that did not meet these requirements were required to have the hard drives removed and degaussed, with the computers (absent the hard drives) sold at auction.

According to INL property records, the computer in question was excessed in June 2004, evaluated by INL personnel and designated to be sold, and placed on a pallet with a number of other computers designated for sale to the public. The pallet of computers was sold in a bulk sale in October 2004. According to DOE officials, after the computer was sold, it came into the possession of an individual with a criminal history, who discovered that the computer's hard drive was still intact and contained unclassified controlled information, including PII. According to DOE officials, the individual retained the hard drive until June 2006, when INL and DOE officials became aware of its existence and recovered it. The previously mentioned criminal investigation did not reveal any evidence of criminal exploitation of the PII data on the hard drive.

INL POLICIES AND PROCEDURES

We also found that BBWI did not revise and implement internal policies and procedures to reflect new requirements in a DOE directive on clearing, sanitizing, and destroying information system storage media, memory devices, and other related hardware that was issued in February 2004. This may have been a contributing factor to the above mentioned improper release of an unsanitized computer containing unclassified controlled information.

DOE Notice 205.12, "Clearing, Sanitizing, and Destroying Information System Storage Media, Memory Devices, and Other Related Hardware," was issued in February 2004 and had a 90-day implementation requirement. The notice was incorporated as a modification into the BBWI contract in May 2004. However, BBWI's internal Management Control Procedure was never modified to incorporate the new requirements of the Notice, which included additional internal controls during the excessing of computers.

DOE Notice 205.12 required the sanitization or degaussing of computer hard drives during the excessing process and that this action be documented, to include the hard drive description, classification level, purpose, and procedure used. In addition, the Notice required computers to be randomly sampled to verify the sanitation or degaussing process was successful prior to the computers leaving a DOE-controlled environment. These requirements were not being followed at INL. If these requirements had been followed, INL might have identified the unsanitized computer before it was sold.

DELAYED POLICY IMPLEMENTATION

We further found that the DOE Idaho Operations Office delayed incorporating DOE Notice 205.12 and its successor directive into the new site management contract with BEA. As a result, INL continued to follow existing internal policies and procedures and did not implement the requirements in the DOE directives for approximately 16 months. This impacted INL's excessing of computers, as discussed above, as well as other electronic equipment with memory devices, such as facsimile and copier machines, which were not being examined prior to excessing to ensure they did not retain data.

We determined DOE Notice 205.12 was not included in BEA's contract when the contract for management of INL was awarded in November 2004. INL continued to operate under the existing internal Management Control Procedure. In June 2005, the Notice was superseded by DOE Manual 205.1-2, "Clearing, Sanitization, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware." However, the Manual was not incorporated into BEA's contract until March 2006. Between November 2004 and March 2006, a period of approximately 16 months, INL continued to operate under the existing internal Management Control Procedure.

We were told by DOE Idaho Operations Office officials that the delay in implementing the DOE policies was due, in part, to INL's management contract change. In late 2003, the Request for Proposal (RFP) to manage INL had been finalized, with the draft RFP being issued on February 4, 2004. Since the Notice was not issued until February 19, 2004, it was not included in the draft RFP. Idaho Operations Office officials told us that their plan was to update the new contract once it was awarded. A review of records indicated BEA was awarded the management contract in November 2004 and that the process for modifying BEA's contract to incorporate the Manual began in January 2005. However, the modification was not completed until March 2006. Subsequently, BEA implemented a new internal policy in May 2006 that incorporated the requirements of the Manual.

SAFEGUARDS FOR HARD DRIVES

During our inspection of internal controls, we also observed that, during the excessing process, INL could improve the physical safeguards provided for computers and other electronic memory devices that potentially contained unclassified controlled information. Specifically, numerous hard drives that INL officials said potentially contained unclassified controlled information were being stored outdoors in a wooden box that could be accessed by unauthorized persons. Other such hard drives were being stored in cardboard boxes within a warehouse area in INL's Personal Computer Redistribution (PCR) Center that could be accessed by non-warehouse personnel. In addition, we observed that computers and computer hard drives that may contain unclassified controlled information were potentially vulnerable to unauthorized access during the excess property receiving process. Additional discussion of these observations is provided below.

Storage of Hard Drives

INL officials told us that, during the computer excessing process, standard sized hard drives were removed and electronically degaussed. However, they said the degaussing machine was not able to degauss older, larger hard drives due to the physical limitations of the machine. Hard drives that could not be degaussed were either placed in cardboard boxes inside the PCR Center, which could be accessed by non-warehouse personnel, or in a wooden box located in an open area outside INL's excess property warehouse, as shown in Picture 1.



Wooden Box Containing Computer Hard Drives
Picture 1

The wooden box was located in a property protection area that was accessible to visitors and others who had access to INL. When we examined the wooden box in July 2006, it was nearly full of hard drives. INL officials told us that the box had recently been bound

with metal straps in preparation for shipping. We noted that, prior to the banding, the only security afforded the box was a hasp and padlock. We also noted that the hasp was secured by external screws that could have been easily removed with a simple instrument, such as a screw driver.

INL officials told us that the box had been outside for at least two years and contained a mixture of degaussed and non-degaussed/non-sanitized hard drives exsessed from INL. INL officials told us that it was possible some of the non-degaussed/non-sanitized hard drives contained unclassified controlled information. The nature of the work performed at INL supports the likelihood of such a possibility.

Transport of Hard Drives

We were told by INL officials that the wooden box and the cardboard boxes in the PCR Center containing the degaussed and non-degaussed/non-sanitized hard drives were in the process of being shipped to Chicago for destruction and recycling. INL officials said that one of the transportation methods being considered was transporting the hard drives in the wooden box and the cardboard containers via an open flat-bed truck. DOE Manual 205.1-2 requires that hard drives must be degaussed or sanitized prior to leaving a DOE-controlled environment. We expressed concern to INL management officials about the storage of the non-degaussed/non-sanitized hard drives and their leaving a DOE-controlled environment. As a result of our concerns, INL management officials reviewed the associated issues and told us that all hard drives had been moved into the excess property warehouse and physically secured pending a final decision on the disposition of the hard drives.

On September 12, 2006, shortly after the completion of our inspection field work at INL, the DOE Chief Information Officer issued a memorandum on “Interim Cyber Security Guidance Concerning Disposal of Computer Storage Media, Including Hard Disk Drives.” It stated that, due to security concerns raised regarding degaussing, no hard disk drive or other magnetic computer storage media or device should be sold, donated, or transferred to an off-site entity for disposal, pending the issuance of new long-term cyber security guidance. Subsequently, we were told by INL management officials that all hard drives would remain physically secured within the excess property warehouse pending the issuance of the new long-term cyber security guidance and its incorporation into INL internal policies and procedures.

Storage of Hard Drives in the Excess Property Warehouse

During a visit to INL's excess property warehouse, we determined that computers and computer hard drives that may contain unclassified controlled information were potentially vulnerable to unauthorized access during the excess property receiving process. We observed that computer equipment waiting to be brought into accountability as part of the receiving process was located within several feet of items awaiting sale to the public as part of an excess property auction. We also observed unescorted non-INL personnel walking around the warehouse among unsanitized computers and hard drives in the receiving area. INL officials told us that, due to the limited number of employees working at the excess property warehouse, computer equipment may remain in the receiving area for as long as two weeks. INL officials also said that the excess property warehouse was a property protection area, with access limited to INL employees and authorized visitors such as potential bidders for auction items and individuals examining equipment for donation. However, INL officials acknowledged that, due to limited staff, once visitors were identified and authorized to enter the warehouse, the visitors were allowed to examine property unescorted, with only general oversight from warehouse employees.

Due to the size of the excess property warehouse, the limited staff, and the multiple access points, it appeared to be very difficult for warehouse personnel to monitor all activities of persons entering the excess property warehouse. We expressed our concerns to INL management about the physical security of computers and memory devices in the receiving area of the excess property warehouse. We were told that a review of the adequacy of the physical security at the excess property warehouse would be conducted to identify possible areas of improvement.

RECOMMENDATIONS

We recommend the Manager, Idaho Operations Office, ensures that:

1. The Idaho Operations Office implements DOE directives into INL management contracts in a timely manner.
2. INL develops and implements physical security policies and procedures to preclude unauthorized access to computers and other memory devices during the excessing process.
3. In the future, INL implements all DOE policy requirements into operational procedures in a timely manner to ensure all excessed memory devices containing unclassified controlled information are properly sanitized, degaussed, or disposed of.

**MANAGEMENT
COMMENTS**

In comments on a draft of our report, management concurred with the recommendations and identified corrective actions that have been or will be taken to address them. Management's comments, excluding minor editorial comments, are included in their entirety at Appendix B.

**INSPECTOR
COMMENTS**

We found management's comments to be responsive to our recommendations. We addressed management's editorial comments as appropriate in the report.

Appendix A

SCOPE AND METHODOLOGY

The field work for this inspection was conducted between July and August of 2006. We interviewed INL and DOE officials and reviewed DOE directives and INL internal policies regarding property management and the excessing of computers and memory devices. We also conducted an on-site evaluation of the operational and internal controls and security of INL's excess property warehouse and INL's PCR Center. We physically examined a number of computers and memory devices at the excess property warehouse and reviewed excess property records and past excess property sale records.

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

United States Government

Department of Energy

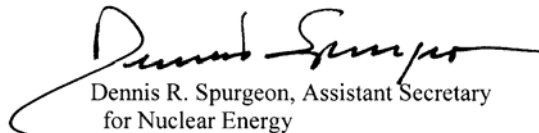
Memorandum

DATE: February 2, 2007
REPLY TO:
ATTN OF: NE-32
SUBJECT: Response to Draft Inspection Report on "Excessing of Computers used for Unclassified Controlled Information at the Idaho National Laboratory"
TO: Christopher R. Sharpely, Deputy Inspector General for Investigations and Inspections, IG-40

Thank you for the opportunity to review and comment on your subject draft report.

We agree with the facts presented, the conclusions reached, and the appropriateness of the recommendations. My office and the Idaho Operations Office concur with the three recommendations. Attachment 1 identifies the corrective actions taken or planned with corresponding schedule dates. Attachment 2 provides four editorial comments on the draft report.

If you have any further questions, please call Owen Lowe at 3-3321.



Dennis R. Spurgeon, Assistant Secretary
for Nuclear Energy

2 Attachments

cc: Elizabeth D. Sellers, ID

Recommendation	Corrective Actions	Planned Completion Date
The Idaho Operations Office implements DOE directives into INL management contracts in a timely manner.	Concur. The Idaho Management System, which recently achieved ISO 9001:2000 certification, includes a Work Instruction (03.WE.03.01) entitled "Identification and Implementation of Directives and Other Departmental Requirements Applicable to the Major Idaho Operations Office Contracts," which requires timely implementation.	Completed 5/30/2006
INL develops and implements security policies and procedures to preclude unauthorized access to computers and other memory devices during the excess process.	Concur. INL has completed changes, in conjunction with the ICP contractor who has been performing this work in support of INL, to limit access to the receiving area of the property disposal facility. In addition, INL is changing the current processes for disposal of computers and other memory devices so that the work is accomplished by INL personnel. Additional specific actions to be completed are: 1) Change the physical location of items staged for receipt actions within the property disposal facility to preclude unauthorized access to computers and other memory devices during excess processing. 2) INL Safeguards and Security will lead the evaluation and improvement of security practices and procedures for control and protection of computer memory devices during the excess process.	3/15/2007 6/30/2007
In the future, INL implements all DOE policy requirements into operational procedures in a timely manner to ensure all excess memory devices containing unclassified controlled information are properly sanitized, degaussed, or disposed of.	Concur. INL is implementing all DOE policy requirements and process improvements in the computer redistribution process to ensure that all excess memory devices containing unclassified controlled information are properly sanitized and disposed of. The computer redistribution area has been isolated from the property disposal area with a locally alarmed access door. Additional specific actions to be completed are: 1) Procure a hard drive and media chipper to destroy all excess memory devices per current DOE guidance.	5/31/2007

Appendix C

PRIOR REPORTS

The following Office of Inspector General reports are related to the excessing of computers and other electronic memory devices.

“Internal Controls for Excessing and Surplusing Unclassified Computers at Los Alamos National Laboratory” (DOE/IG-0734, July 2006). This report found that Los Alamos did not follow DOE directives and internal policies pertaining to excessing computers. As a result, an excessed computer with an intact, unsanitized hard drive was sold to the public. Further, the internal control failure relating to the excessing and surplusing of this computer raised concerns as to whether the hard drives for seven other computers excessed at the same time were sanitized and removed prior to the computers being sent to auction.

“Destruction of Classified Hard Drives at Sandia National Laboratory-New Mexico” (DOE/IG-0735, August 2006). This report found that Sandia did not destroy classified computer hard drives in accordance with DOE directives. Sandia did not always maintain proper documentation, destroy hard drives on the same day they were removed from the site, obtain proper approval for off-site destruction of hard drives, and use appropriately cleared personnel for the destruction process.

“Excessing of Computers Used for Unclassified Controlled Information at Lawrence Livermore National Laboratory” (draft). This report found that for over two years the National Nuclear Security Administration (NNSA) delayed implementing at Lawrence Livermore National Laboratory (LLNL) two DOE directives that provided guidance on clearing, sanitizing, and destroying unclassified controlled memory devices. Further, the report found that NNSA’s delay in implementing the policies at LLNL negatively impacted the way LLNL excessed computers and memory devices.

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?
2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?
3. What format, stylistic, or organizational changes might have made this report's overall message clearer to the reader?
4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?
5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Judy Garland-Smith at (202) 586-7828.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
<http://www.ig.doe.gov>

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.