United States General Accounting Office

GAO

Report to the Ranking Minority Member, Committee on Governmental Affairs, U.S. Senate

June 1995

DEPARTMENT OF ENERGY

Procedures Lacking to Protect Computerized Data

RESTRICTED--Not to be released outside the General Accounting Office unless specifically approved by the Office of Congressional Relations.

RELEASED

GAO/AIMD-95-118

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-258977

June 5, 1995

The Honorable John Glenn
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

Dear Senator Glenn:

This report responds to your request for information regarding an alleged sale of surplus Department of Energy (DOE) computer equipment to an Idaho businessman. Specifically, you asked us to determine whether (1) the computer sale actually took place and (2) any surplus computers sold to this businessman contained classified or sensitive unclassified information.[1] You also asked us to determine whether DOE is subject to Federal Information Resources Management Regulation (FIRMR) Bulletin C-22, which provides guidance on the security and privacy protection of federal computer resources.

Results in Brief

Between April 1, 1993, and September 30, 1994, DOE's Idaho National Engineering Laboratory (INEL) sold at least 25, but perhaps as many as 50, surplus personal computers to a salvage dealer located in Pocatello, Idaho. We could not confirm the actual number of computers sold because INEL is not required to document the identities of purchasers of all categories of surplus automated data processing (ADP) equipment. In addition, the salvage dealer did not maintain complete records of computers purchased.

Sales and inventory records for the 25 computers that we could trace to the salvage dealer did not indicate that any of these computers had been designated or used to process classified data. However, we could not determine whether other computers sold to the salvage dealer contained classified data because we could not account for or examine all computers sold.

A review by the DOE Idaho Operations Chief Information Officer concluded that some of the computers sold to the salvage dealer may have contained sensitive data, but did not determine how many. The review reached this conclusion primarily because DOE's contractors involved in excessing

[1]DOE Order 1360.2B defines sensitive unclassified information as data that require protection because of statutory or regulatory restrictions, or because inadvertent or deliberate misuse, alteration, disclosure, or destruction could adversely affect national or other DOE interests.

computers that may have contained sensitive data did not have written procedures explaining how to properly sanitize the computers.

At our request, DOE officials reviewed information regarding contractor personnel who used the 25 computers that could be traced to the salvage dealer. The officials told us that they could only offer positive assurance that 11 of the computers were not used to process classified or sensitive data. We examined the contents of the hard drives on four of the total quantity of computers sold to the salvage dealer, and found numerous data files related to DOE's spent nuclear fuel and radioactive waste management activities. However, security and program management officials at the Idaho Operations Office and INEL reviewed these data and determined that they were not sensitive.

FIRMR Bulletin C-22 states that federal agencies, including DOE, should establish security safeguards and procedures to ensure the proper disposition of sensitive automated information. Although DOE has distributed Bulletin C-22 to its field and operations offices, it has not taken actions to ensure that provisions of the Bulletin are being implemented, and that all excess computers are properly sanitized.

Background

INEL was established in 1949 as the National Reactor Testing Station to develop commercial applications of nuclear power. It currently performs systems integration and engineering, research and development, and project management to support environmental cleanup and waste management, energy production and use, economic competitiveness, and national security activities. INEL is the lead engineering laboratory for new technologies, and serves as the applied engineering laboratory for the entire DOE complex.

INEL is administered by DOE's Idaho Operations Office. Until September 1994, its work was performed by five separate management and operating contractors—EG&G Idaho, Inc.; Westinghouse Idaho Nuclear Company, Inc.; Babcock and Wilcox Idaho, Inc.; MK-Ferguson Company; and Protection Technology Idaho, Inc. In October 1994, these contractors were replaced by the current contractor, Lockheed Idaho Technologies Company.

DOE's property management instructions state that property offices must report all property that is no longer needed, including ADP equipment, as excess. DOE's order on unclassified computer systems further states that

all sensitive unclassified automated information must be appropriately protected from unauthorized access or disclosure, and tasks the Director of Information Resources Management with developing and implementing Departmental policies and procedures for protecting the transmission of such information.

Idaho Operations officials stated that at the time of the computer sales, the INEL contractors were supposed to transfer unneeded ADP equipment to a property handling facility known as the "PC Store." This facility was responsible for determining whether the equipment was reusable or excess, and was supposed to erase any data left on the hard disk drives. Equipment declared excess was then forwarded to an excess warehouse for donation or public sale.

In accordance with Federal Property Management Regulations, DOE's excess property is designated in two categories—reportable and nonreportable. At the time of the computer sales, INEL contractors considered excess property as being reportable to DOE if its acquisition cost was more than $1,000 and if the property was less than 8 years old. DOE sales records for reportable property contain information identifying the purchasers of excess equipment; however, DOE sales records for nonreportable property do not contain information identifying purchasers. INEL documents showed that between April 1, 1993, and September 30, 1994, its contractors excessed over 900 items of ADP property, including 185 pieces of reportable equipment and 723 pieces of nonreportable equipment.

Scope and Methodology

To address our objectives, we interviewed DOE headquarters and Idaho Operations Office officials responsible for property and information resources management; staff in DOE's inspector general's office; and representatives of Lockheed Idaho Technologies Company. We also interviewed several employees who formerly worked for EG&G Idaho, Inc. However, we did not interview other representatives of the five contractors operating INEL when the computers were sold because DOE had terminated its contracts with them.

To determine the quantity of computers sold and whether any of the computers contained classified or sensitive data, we reviewed INEL's inventory tracking reports and sales records for all excessed ADP equipment between April 1, 1993, and September 30, 1994. In addition, we reviewed Bulletin C-22 and directives detailing DOE Headquarters and

Idaho Operations Office requirements for the security and disposition of excess computer resources.

We also interviewed the Idaho salvage dealer and several individuals to whom the salvage dealer subsequently resold the computers. Finally, we examined the contents of the hard drives on four of the computers sold to the salvage dealer (three computers that the salvage dealer had not disassembled or resold and one computer that had been purchased by a local citizen that we could identify). We could only examine four of the total quantity of computers sold to the salvage dealer because he had either disassembled the other computers or resold them to individuals not identified in his sales records.

We performed our work between October 1994 and March 1995 in accordance with generally accepted government auditing standards. We requested comments on a draft of this report from the Secretary of Energy or her representative. On May 8, 1995, officials at the Department of Energy, including the Director of the Office of Contractor Management and Administration, provided oral comments. These comments are discussed in the "Agency Comments and Our Evaluation" section.

Computers Were Sold but Quantity Cannot Be Determined

Between April 1, 1993, and September 30, 1994, DOE's INEL sold at least 25, but perhaps as many as 50, surplus personal computers to a salvage dealer located in Pocatello, Idaho. INEL documents of its reportable computer sales showed that the salvage dealer purchased 25 personal computers. However, the salvage dealer told us that he purchased approximately 50 personal computers.

We could not determine exactly how many computers were sold because the items that were sold included both reportable and nonreportable ADP equipment, and the records of nonreportable property sales do not identify purchasers. In addition, the salvage dealer did not maintain records of all of his computer purchases. He also told us that most of the computers had already been sold or disassembled, making it impossible to accurately count his inventory. According to the salvage dealer, working parts from some systems were used to replace nonworking parts in other systems. The salvage dealer estimated that through this process, he had rebuilt and sold about 30 computers to students and other local businesses.

Classified and Sensitive Data May Have Been Compromised

We examined sales and inventory tracking records for the 25 computers that could be traced to the salvage dealer. We also examined the contents of the hard drives on four of the computers that were sold to the salvage dealer.[2] In both instances, we did not find any information indicating that the computers had been designated or used to process classified data. DOE's Office of Inspector General also reviewed information and computers related to the computer sales and determined that classified data had not been compromised.

DOE directives provide specific guidance for handling computers used to process classified data.[3] Included in this guidance are requirements for conspicuous external labels to indicate the highest classification level of data processed, and for sanitization of the storage media, memory, and hardware. An Idaho Operations official stated that, in accordance with the approved procedures, every classified computer is sanitized prior to disposal. However, we could not determine whether some of the computers sold to the salvage dealer contained classified data because most of the computers could not be accounted for or examined.

INEL contractors could also have sold computers containing sensitive data. A review by the DOE Idaho Operations Chief Information Officer determined that sensitive data may have been left on some of the computers because the contractors involved in excessing the computers did not have written procedures explaining how to properly sanitize the computers. However, the review did not indicate how many of the computers may have contained sensitive data.

At our request, DOE officials reviewed information regarding the contractor personnel who used the 25 computers that were traced to the salvage dealer. The officials could only offer positive assurance that 11 of the computers had not been used to process classified or sensitive data; they did not have sufficient information to determine whether the remaining 14 computers had processed classified or sensitive data.

During our examination of four of the computers that were sold to the salvage dealer, we found numerous files containing data about DOE's programs and activities. For example, we found data files identifying

[2]The four computers were among the total quantity of reportable and nonreportable computers sold to the salvage dealer.

[3]DOE 5639.6A, Classified Automated Information System Security Program, and DOE M5639.6A-1, Manual of Security Requirements for the Classified Automated Information System Security Program, July 15, 1994.

storage locations and estimated inventories of spent nuclear fuel at DOE sites, as well as plans related to the management and disposal of high-level radioactive waste. We provided these data to Idaho Operations officials and asked them to determine whether any of these data were classified or sensitive. In its response, the Idaho Operations Office stated that a joint review of the data by the Unclassified Computer Security Coordinator, the Spent Fuel Program Manager, and INEL's Chemical Process Plant Facility Manager, had determined that the data were not sensitive.

According to the review by the Chief Information Officer, the contractors involved in excessing computers that may have contained sensitive data did not have (1) written ADP equipment excessing procedures or (2) the equipment needed to effectively sanitize the hard drives. The report also noted that all of the contractors did not follow the same process for transferring ADP equipment to the excess warehouse. For example, some of the contractors sent their equipment to the PC Store, while others transferred it directly to the excess warehouse. The only way that the excess warehouse could know whether equipment it received had been sanitized was if annotations in the inventory tracking reports or markings affixed to the equipment indicated so.

We reviewed approximately 900 inventory tracking reports for excessed ADP equipment and found only 10 annotated to state that the hard drives had been erased or removed. We also examined computers held in the excess warehouse and by the salvage dealer, and saw no markings affixed to any equipment indicating that it had been sanitized.

DOE Idaho Operations officials stated that because of the questions raised regarding the computer sales, they have implemented various measures aimed at preventing the improper disclosure of sensitive data processed on their computers. For example, on August 4, 1994, the Idaho Operations Office placed a moratorium on the disposal of all INEL surplus property. In addition, the Office has issued policy statements stipulating that all ADP equipment should be purged of all information processing software and data prior to being excessed. However, these policy statements do not contain specific guidance stating how to sanitize the ADP equipment.

DOE Is Subject to FIRMR Bulletin C-22

FIRMR Bulletin C-22 states that federal agencies, including DOE, should establish internal procedures to ensure the proper disposition of sensitive automated information. The Bulletin, issued in September 1992 and supplemented in July 1994, also provides that agencies should ensure that

contractors acting on their behalf maintain adequate security at their installations. The procedures for the proper disposition of sensitive automated information include completely removing the sensitive data by either magnetically erasing it from the disk storage media using approved equipment or by destroying the storage media.

An official in DOE's Office of Information Management told us that they are aware of Bulletin C-22, and that they have distributed the Bulletin to the field and operations offices for their use. The official also told us that they included information about the Bulletin in DOE's draft Information Systems Security Program Manual, and have incorporated language requiring the sanitization of excess ADP equipment in DOE's draft property management regulations and interim policies for controlling high-risk property. However, the official also stated that each office has discretion in how it chooses to implement the Bulletin, and that DOE has not taken actions to ensure that provisions of the Bulletin are being implemented. In addition, DOE officials stated that field and operations offices do not have procedures that instruct all contractors on how to properly dispose of excess ADP equipment, and that they cannot ensure that all excess computers are properly sanitized.

Conclusions

Although our reviews of sales records and some of the computers sold to the salvage dealer did not reveal any specific instances in which classified or sensitive data were compromised, DOE's Idaho Operations Office and INEL may have compromised the security of such data by not ensuring that all excess computers were adequately sanitized. DOE's Idaho Operations Office has begun implementing measures aimed at preventing disclosures of sensitive systems and data, and the Office of Information Management has distributed FIRMR Bulletin C-22 to operations and field offices. However, these offices have discretion in how they choose to implement the Bulletin, and DOE has not ensured that it is being implemented. In addition, procedures that instruct all contractors on how to properly dispose of excess ADP equipment have not been established. As a result, DOE operations continue to be at risk of not adequately securing sensitive data.

Recommendation

We recommend that the Secretary of Energy direct the Deputy Assistant Secretaries for Information Management and for Procurement and Assistance Management to develop and implement procedures in DOE's operations and field offices that instruct all contractors on the proper

disposal of excess ADP equipment. These procedures should include instructions on how contractors should properly sanitize excess computers. The Secretary should then require all operations and field offices to adhere to these procedures when disposing of excess ADP equipment.

Agency Comments and Our Evaluation

DOE officials, including the Director of the Office of Contractor Management and Administration, provided oral comments on a draft of this report. The officials generally concurred with the report's findings, but disagreed with certain facts and characterizations. Specifically, the officials disagreed with our position that classified data may have been compromised through the sale of surplus computers. They stated that our overall discussion of this issue was misleading and that it portrayed INEL as having sold computers that contained classified data because it could not prove otherwise. The officials stated that it would be more appropriate to assume that no computers containing classified data were sold because (1) Idaho Operations officials told us that all computers used to process classified data were sanitized in accordance with established procedures and (2) we did not identify any computers containing classified data during our review.

We have revised the report to more clearly present our discussion on classified data. However, we disagree with the position that we should assume that no computers containing classified data were sold. Although Departmental procedures provide specific guidance for handling computers used to process classified data, Idaho Operations Officials were unable to determine whether or not some of the computers sold had processed classified data. The lack of Departmental assurance that all computers were properly sanitized prior to being excessed increases the possibility that computers containing both classified and sensitive data may have been sold.

The officials also expressed concern that the report did not recognize actions that DOE has taken to implement FIRMR Bulletin C-22. The officials highlighted several efforts, including (1) issuance of the Bulletin to DOE's operations and field offices, (2) discussion on the Bulletin in DOE's draft Information Systems Security Program Manual, and (3) incorporation of language requiring the sanitization of excess ADP equipment in DOE's draft property management regulations and its interim policies for controlling high-risk property. While we agree that these efforts are good first steps toward ensuring proper and adequate sanitization of excess ADP

equipment, DOE's field and operations offices still have not implemented procedures to ensure that all contractors properly dispose of excess ADP equipment. Without these procedures, DOE cannot ensure that its operations adequately secure sensitive data.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days after the date of this letter. At that time, we will send copies of this report to the Secretary of Energy and to appropriate congressional committees. Copies will also be made available to others upon request.

Please call me at (202) 512-6253 if you or your staff have any questions. Major contributors to this report are listed in appendix I.

Sincerely yours,

Joel C. Willemssen
Director, Information Resources
Management/Resources, Community,
and Economic Development

Contents

Letter 1

Appendix I Major Contributors to This Report 12

Abbreviations

ADP	automated data processing
DOE	Department of Energy
FIRMR	Federal Information Resources Management Regulation
INEL	Idaho National Engineering Laboratory

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Valerie C. Melvin, Assistant Director Shirley E. Todd, Senior Auditor Keith Rhodes, Technical Assistant Director
Denver Regional Office	Peter Fernandez, Evaluator-in-Charge
Office of the General Counsel	John A. Carter, Senior Attorney

[illegible]

[illegible] is free. [illegible] sent to the [illegible] check or money order [illegible] should be mailed to a [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) [illegible] or TDD (301) 413-0006.

Each day GAO issues a list of [illegible] reports and testimony. To receive [illegible] copy of the daily list or any list from the past 30 days, please call (202) [illegible] using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Mail
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested