U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

Management of Sensitive Equipment at Selected Locations

DOE/IG-0606

June 2003

Department of Energy

Washington, DC 20585

June 16, 2003

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Management of Sensitive Equipment at Selected Locations"

BACKGROUND

The Department of Energy and its facilities' management contractors have come under increased scrutiny regarding the management of sensitive personal property. The Department defined sensitive property as equipment susceptible to misappropriation for personal use or readily convertible to cash. Generally, this includes equipment such as computers, personal digital assistants, cameras, and communications equipment. The Department has made a significant investment in sensitive property. For example, our analysis of inventory records at the Lawrence Berkeley and Lawrence Livermore National Laboratories and the Stanford Linear Accelerator Center disclosed that the acquisition cost of their active sensitive property inventories exceeded $152 million.

Because of the importance of this issue, we initiated an audit at these sites to determine whether the Department was properly managing sensitive equipment.

RESULTS OF AUDIT

Management was ultimately able to locate virtually all of the items of sensitive equipment we sampled. However, locating the equipment required a level of effort by management which, in our judgment, exceeded normal expectations. The review suggested a number of opportunities to improve accountability of sensitive equipment. For example:

- Each site had sensitive items that had not been properly marked as Government property;
- Property records were not always updated to reflect custody changes when employees were reassigned or terminated;
- Berkeley and Stanford did not always apply inventory controls to computers that were fabricated on site;

- Even though Berkeley purchased and maintained significant amounts of sensitive property, it was permitted to restrict inventory controls to a single class of property -- computers; and,

- Sites did not always ensure that items reported as stolen were entered into law enforcement recovery databases.

Further, we found that Department officials did not always ensure that contractors consistently complied with local guidance and best practices pertaining to control, tracking, and protection of sensitive property.

While almost all sample items were eventually located, recent agency experience suggests that the Department would be well served if controls over sensitive equipment were strengthened, improving accountability and deterring possible misuse, theft, or other diversion of Government property.

Management at the laboratories recognized the concerns raised during this review and indicated that they intended to address the issues. For example, officials from Livermore and Berkeley informed us that they planned to develop uniform sensitive property control and accountability techniques. This is a positive step. However, the report includes additional recommended actions designed to strengthen the protection of sensitive Government property.

MANAGEMENT REACTION

Departmental managers concurred with our recommendations and cited specific actions taken to strengthen controls over sensitive equipment.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary for Energy, Science and Environment
Associate Administrator for Management and Administration, NNSA
Director, Office of Science
Director, Office of Resource Management, Office of Management, Budget and Evaluation/Chief Financial Officer

MANAGEMENT OF SENSITIVE EQUIPMENT AT SELECTED LOCATIONS

TABLE OF CONTENTS

SENSITIVE EQUIPMENT ACCOUNTABILITY

Opportunities for Improvements of Property Management Controls

While sites were ultimately able to locate virtually all of the items of sensitive equipment we sampled, we noted opportunities to improve controls and accountability. For example, we observed overly restrictive definitions of sensitive equipment and failures to follow local guidance and best practices for the control, tracking, and protection of sensitive property.

Sensitive Equipment

The United States Code of Federal Regulations (CFR), Section 41, Chapter 109, through which Departmental property regulations are implemented, defines sensitive items as "property susceptible to being appropriated for personal use or which can be readily converted to cash." Cited as examples of items that should be closely controlled are portable photographic equipment, communications equipment, portable power tools, as well as laptops and other computers. Contractors are required to obtain Departmental approval for the types of property to be treated as sensitive.

Despite the wide range of equipment contemplated by regulation, the Department of Energy (Department) permitted the Lawrence Berkeley National Laboratory (Berkeley) to restrict sensitive equipment tracking and control only to computers. The restrictive definition was further narrowed in that it applied only to laptops and desktop computers and excluded all other related peripherals such as printers, monitors, and scanners. While Berkeley justified its decision, and received approval from local Departmental officials, the analysis supporting the decision did not adequately consider the inherent risk associated with sensitive equipment.

Berkeley believed that low loss figures developed during previous inventories and the declining cost of electronic equipment in general justified narrowing the definition. The analyses did not, however, adequately address inherent risk of loss and the deterrent effect associated with strong accountability and inventory controls. Because controls had not been applied in this area, a significant amount of effort, and delays as long as 10 days, were required for Berkeley property management officials to identify property that we selected for inventory testing. Delays and difficulties in locating property were noted for a number of items cited in the CFR and was not limited to computers.

Equipment Tagging

Despite Departmental and local property guidance, we observed that sensitive property was not always marked or properly identified as Government property. Each of the three locations reviewed required the use of Government property stickers on items such as computer monitors and cellular telephones, and in some cases, even noted the theft deterrent associated with such marking. However, we noted that such requirements were not routinely followed and that numerous items had not been properly marked. Property management officials at Berkeley told us that they were not actively pursuing tagging what they considered "non inventory" items. At Stanford Linear Accelerator Center (Stanford), we also identified three sensitive items that were not tagged and tracked as required.

We also noted that inventory stickers were not always affixed to computers that had been assembled from components at the site. In spite of requirements to tag and track fabricated property items, we observed that approximately 40 computers assembled at Berkeley and 3 at Stanford did not have inventory stickers and were not listed in the property system. Based on our sampling, this problem appears to be limited primarily to computers assembled on site.

Property Records

In addition, inventory records did not always accurately reflect either the correct custodian or location of sensitive property. Specifically, we found instances where employees were relocated or equipment was reassigned, and inventory records were not updated to reflect the change. For example, a sample of 150 recently terminated employees revealed that 17 still had 41 pieces of active sensitive equipment assigned to them. Berkeley and the Lawrence Livermore National Laboratory (Livermore) told us after completion of our site work that they had been able to locate all of the items of equipment in question. Stanford, however, was unable to locate several items.

The sites, in many instances, were only able to locate the items in our samples after extensive effort. In certain instances, we had limited assurance that items such as computer monitors and printers observed during our testing were the actual items of interest. This occurred because at each of the sites certain items of sensitive equipment were not included in inventory, and procurement records did not contain serial or specific model numbers. In those cases, we relied on product description, manufacturer, or similar information in an attempt to distinguish the sampled item among like items.

Law Enforcement Databases

Site officials also did not always take advantage of opportunities to report stolen property to national law enforcement databases, which may have increased the likelihood of regaining control of recovered stolen property. At Livermore, site law enforcement officials told us that they reported property stolen on-site to the National Crimes Information Center (NCIC). However, officials at Berkeley and Stanford indicated that law enforcement officials authorized to access the NCIC database were no longer employed at their sites and thus property stolen on-site was not reported to NCIC. In addition, site officials stated that they did not always coordinate with local law enforcement to ensure that property stolen off-site is entered in the NCIC database. We noted that of the 47 sensitive items stolen on or off the three sites over the past two years, only 9 had been entered into the NCIC database. Without such entries, even if the items were subsequently recovered it is unlikely they would be returned to the Government.

Other Control Issues

During our review, several other issues were identified that detract from the effectiveness of property control efforts. Specifically:

- Weaknesses in controls over the delivery of sensitive equipment increased the risk that equipment could be stolen or removed by other than the intended recipient. While the delivery of most equipment was properly controlled, at Livermore, equipment could be dropped off at facilities and left unsecured without a custodian signing for the property. At Stanford, sensitive equipment could be delivered directly to an end user without first being entered into the property accounting system;

- None of the sites reviewed maintained accountability over sensitive property until final disposition. Equipment that had reached its full service life was removed from the inventory management system regardless of whether it remained in use. For example, at Livermore, accountability was not maintained for computers that were over 5 years old. Such equipment was not subjected to periodic inventory and custody/location changes were not recorded; and

- Controls over property used off-site were not consistently enforced. In several instances, property was removed from the site without first obtaining a property pass.

Property Standards and Implementation Procedures

These weaknesses occurred because the Department did not ensure that contractors consistently complied with local guidance and best practices pertaining to control, tracking, and protection of sensitive property, and in the case of Berkeley, permitted the site to adopt a narrow definition of sensitive equipment. Inconsistent implementation of inventory control procedures also resulted in sensitive equipment not being properly tagged and tracked throughout its lifecycle. The Department also permitted Berkeley to limit its control of sensitive equipment to computers, thus excluding accountability for highly attractive items such as digital cameras, personal digital assistants, and video equipment that are easily pilfered.

Control Environment

While the sites reviewed were ultimately able to locate virtually all of the items included in our samples, opportunities to improve controls and accountability over sensitive property exist. As noted in our recent special inquiry at Los Alamos, weak property accounting controls had a serious and substantial impact on operations of the Laboratory and severely damaged its reputation. The Department should ensure that all sensitive property is properly identified and that management controls are in place and are operating as intended. Without improvements in this area, sites remain susceptible to misuse, theft, or other diversion of Government property.

RECOMMENDATIONS

To ensure sensitive equipment is adequately managed, we recommend the Associate Administrator for Management and Administration, NNSA and the Director, Office of Science, in conjunction with the Director, Office of Resource Management, Office of Management, Budget and Evaluation:

1. Provide guidance to specifically define the categories of sensitive equipment to be accounted for by contractors; and,

2. Ensure that contractors follow sound property accounting management practices including:

   - Properly identifying sensitive items;
   - Coordinating with local law enforcement agencies to ensure that stolen property is entered into the national stolen property database; and,
   - Maintaining current site inventory property records including control over the delivery, receipt, and movement of sensitive equipment.

MANAGEMENT REACTION

Management generally agreed with the draft report and recommendations. Specifically, management agreed that there were opportunities to improve controls and accountability over property and cited specific actions initiated to realize these opportunities. For example, management stated that it had taken action to clarify roles and responsibilities, strengthen accountabilities, and review business systems that purchase, track, and manage sensitive property. Management also provided technical comments on the draft that we considered in preparing the final report.

AUDITOR COMMENTS

Management's comments are responsive to our recommendations.

Appendix 1

OBJECTIVE

The objective of this audit was to determine whether the Department was properly managing sensitive equipment at selected sites.

SCOPE

The audit was performed between December 2002 and March 2003 at the Lawrence Berkeley National Laboratory in Berkeley, California; the Lawrence Livermore National Laboratory in Livermore, California; and the Stanford Linear Accelerator Center in Palo Alto, California.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and regulations pertaining to sensitive equipment management. We also reviewed reports by the Office of Inspector General, the General Accounting Office, and contractor internal audit organizations;
- Reviewed the *Government Performance and Results Act of 1993* and determined if performance plans and measures had been established;
- Reviewed numerous documents related to property management and procurement;
- Conducted inventory verification of statistical samples of sensitive items. Because site definitions for sensitive equipment varied, we used data mining techniques to identify the populations of sensitive equipment purchases at each site. We then statistically selected samples from these populations. In all, we sampled 1,537 items for verification. Firearms and ammunition were excluded from our examination because they were addressed in our recently issued report on *Inspection of Firearms Internal Controls at Los Alamos National Laboratory* (DOE/IG-0587, February 2003); and,
- Held discussions with program officials and personnel from Headquarters, Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, Oakland Operations Office, and Stanford Linear Accelerator Center.

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objectives. Accordingly, we assessed internal controls regarding the management of sensitive equipment. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did rely on computer-processed data to accomplish our audit objectives. We performed limited test work of data reliability during our audit and determined we could rely on computer-processed data.

Management waived the exit conference.

Appendix 2

PRIOR AUDIT REPORTS

- *Interim Report on Inspection of Internal Controls Over Personal Computers at Los Alamos National Laboratory*, (DOE/IG-0597, April 2003). The purpose of this inspection was to determine the adequacy of internal controls over laptop and desktop computers at Los Alamos. The inspection found that controls over classified and unclassified laptop computers were inadequate. Specific recommendations were made to improve controls. Management, while not formally concurring, expressed general agreement with the report, and stated that the issues presented in the report would be factored into corrective action efforts underway by the University of California, Los Alamos National Laboratory, and others.

- *Inspection of Firearms Internal Controls at Los Alamos National Laboratory* (DOE/IG-0587, February 2003). Significant internal control weaknesses exist in the receiving process and the administration of the firearms inventory. Specifically, Los Alamos officials were unable to provide an accurate firearms inventory; some firearms were not entered into the inventory; site inventory validations did not identify inaccuracies; separate firearms inventories maintained by the Laboratory and its protective force contractor were not reconciled; and, all firearms were not processed through a central receiving point. These weaknesses increase the vulnerability of firearms to loss, theft, and abuse.

- *Special Inquiry on Operations at Los Alamos National Laboratory* (DOE/IG-0584, January 2003). The inquiry disclosed a series of actions by Laboratory officials that had the effect of obscuring serious property and procurement management problems and weakened or overrode relevant internal controls. Specifically, there was inadequate or untimely analysis of, and inquiry into, property loss or theft and security issues; lack of personal accountability for property; a substantial degree of dysfunction in the Laboratory's communication and assignment of responsibilities for the handling of property loss and theft concerns; and, inadequate controls over procurement and property systems.

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0580, December 2002). Based on ongoing work at Los Alamos National Laboratory, the OIG observed a substantial degree of dysfunction in the Laboratory's handling of property loss and theft. The OIG and other reviewers identified significant weaknesses in internal controls over property and the use of purchase cards.

- *Inspection of Lawrence Livermore National Laboratory Credit Card Usage and Property Management Concerns* (INS-O-01-01, February 2001). Improvements could be made in the property management process at Lawrence Livermore National Laboratory. Specifically, Livermore could have expanded its list of personal property items considered to be sensitive with regard to items frequently purchased with credit cards. In addition, some credit card users in eight of Livermore's ten Directorates included in the inspection were not identifying personal property items purchased with credit cards as U.S. Government property as required by contract.

- *Department of Energy Management of Excess Property* (GAO/RCED-99-3, November 1998). Neither federal property management regulations nor the Department's regulations and guidance include specific criteria to determine when personal property is no longer needed. Most of the Department's real and personal property are under the control of its contractors. The Department acknowledged problems with its identification and disposal of excess real and personal property.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

MAY 13 2003

MEMORANDUM FOR Frederick D. Doggett
Deputy Assistant Inspector General
for Audit Services

FROM: Michael C. Kane
Acting Associate Administrator
for Management and Administration

SUBJECT: Comments to IG's Draft Report on the Management of Sensitive Equipment

NNSA appreciates having had the opportunity to have reviewed the Inspector General's (IG) draft report, "Management of Sensitive Equipment at Selected Locations." The locations for the audit were the Lawrence Berkeley and Lawrence Livermore National Laboratories and the Stanford Linear Accelerator Center. The Lawrence Livermore National Laboratory is an NNSA laboratory while the other two locations are under the cognizance of the Department's Office of Science.

While the Office of Science is providing a separate response, NNSA agrees that, as the IG states, there are always opportunities to improve controls and accountability over any property. NNSA believes, and I interpret the draft to support, that sensitive equipment is being properly managed but needs to be strengthened. We appreciate the fact that the IG acknowledges their planned development of uniform sensitive property control and accountability changes. We also agree with the IG that controls over sensitive property must be strengthened.

Since all locations are contractually managed by NNSA's Livermore Site Office, we asked the staff to prepare some comments for NNSA's and the Office of Science's consideration. I am providing those comments to you for your consideration prior to issuance of the final report.

Should you have any questions, please contact Richard Speidel, Director for Policy and Internal Controls Management. He may be reached at 202-586-5009.

cc: Director, Office of Science, SC-1
Senior Procurement Executive, NA-63

Printed with soy ink on recycled paper

Department of Energy
Office of Science
Washington, DC 20585

Office of the Director

May 16, 2003

MEMORANDUM FOR FREDERICK D. DOGGETT
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDIT SERVICES

FROM: RAYMOND L. ORBACH
DIRECTOR
OFFICE OF SCIENCE

SUBJECT: Comments on IG Draft Report, "Management Sensitive Equipment at Selected Locations"

Staff of the Office of Science and the Office of Management, Budget and Evaluation have reviewed the subject report and offer the following comments.

Management agrees in general with the recommendations, and already has in process actions that will result in improvements in how sensitive equipment is managed and controlled at field sites. Since 2002, the Department's Office of Contract and Resource Management has been working with the General Services Administration to revise and clarify the definition of "sensitive items" to include now commonplace, commercially available items such as Personal Digital Assistants and cell phones. Pursuant to the President's Management Agenda, SC and NNSA have undertaken restructurings of their respective national organizations so that roles and responsibilities are clear and authorities and accountabilities are strengthened; the restructurings will result in uniformity in policies and procedures in the proper identification of sensitive property and in the purchasing, tracking, and management of sensitive property across SC and NNSA sites; the restructurings should also make it possible to share easily best practices across sites. Finally, the Office of Science, working with the Office of Management, Budget and Evaluation, is in the process of testing its business systems at each of its laboratories (save two which are already undergoing GAO audits) to ascertain any potential vulnerability and associated risks for abuse. Systems employed for the purchase, tracking, and management of personal, sensitive property, are to receive special attention.

IG Report No.: DOE/IG-0606

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 audit 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 this report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

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 Wilma Slaughter at (202) 586-1924.

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.