Department of Energy
Washington, DC 20585

January 3, 2007

Re: Freedom of Information Act Request F2006-00706

This is the Office of Inspector General (OIG) response to your request for information that you sent to the Department of Energy (DOE) under the Freedom of Information Act (FOIA), 5 U.S.C. 552. You asked for a copy of a report entitled "Memorandum to the Secretary, Selected Controls over Classified Information at the Los Alamos National Laboratory," dated November 27, 2006.

The OIG has completed the search of its files for the document responsive to your request. A review of the responsive document and a determination concerning its release has been made pursuant to the FOIA, 5 U.S.C. 552. Certain information has been withheld pursuant to subsections (b)(2), (b)(5), (b)(6) and (b)(7)(C) of the Act, or Exemptions 2, 5, 6, and 7(C), respectively.

Exemption 2 protects from disclosure records "related solely to the internal personnel rules and practices of an agency." This exemption encompasses two categories of information that may be protected from disclosure. One of the categories is information of substantial internal matters, the disclosure of which would risk circumvention of a statute or agency regulation. Information of this nature is referred to as "High 2."

The "High 2" information has been withheld from the documents because of the need to protect sensitive information systems and other critical infrastructures at DOE. This information may reveal current vulnerabilities of systems, installations, infrastructures or projects relating to national security and should be protected from potential security breaches and harm. For this reason, the information is exempt from disclosure pursuant to Exemption 2.

Exemption 5 exempts from mandatory disclosure "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency. . . ." Exemption 5 incorporates the deliberative

process privilege which protects recommendations, advice, and opinions that are part of the process by which agency decisions and policies are formulated.

The information redacted under Exemption 5 reflects the advisory opinions from subordinates. The OIG has determined that the disclosure of material withheld pursuant to Exemption 5 is not in the public interest. In this case, the disclosure of predecisional deliberative material would inhibit frank and open discussion of the matter and would hinder the Government's ability to reach sound and well-reasoned solutions.

Exemption 6 protects from disclosure "personnel and medical and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. . . ." ." Exemption 7(C) provides that "records or information compiled for law enforcement purposes" may be withheld from disclosure, but only to the extent the production of such documents "could reasonably be expected to constitute an unwarranted invasion of personal privacy. . . ."

Names and information that would tend to disclose the identity of certain individuals have been withheld pursuant to Exemptions 6 and 7(C). Individuals involved in the OIG enforcement matters, which in this case include subjects, witnesses, sources of information, and other individuals, are entitled to privacy protections so that they will be free from harassment, intimidation and other personal intrusions.

To the extent permitted by law, the DOE, in accordance with Title 10, Code of Federal Regulations (C.F.R.), Section 1004.1, will make available records it is authorized to withhold pursuant to the FOIA unless it determines such disclosure is not in the public interest.

In invoking Exemptions 6 and 7(C), we have determined that it is not in the public interest to release the withheld material. In this request, we have determined that the public interest in the identity of individuals who appear in these files does not outweigh these individuals' privacy interests. Those interests include being free from intrusions into their professional and private lives.

As required, all releasable information has been segregated from the material that is withheld and is provided to you. See 10 C.F.R. 1004.7(b)(3).

This decision may be appealed within 30 calendar days from your receipt of this letter pursuant to 10 C.F.R. 1004.8. Appeals should be addressed to the Director, Office of Hearings and Appeals, HG1/L'Enfant Plaza Building, U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, DC 20585-1615.

Thereafter, judicial review will be available to you in the federal district court either (1) in the district where you reside, (2) where you have your principal place of business, (3) where the Department's records are situated, or (4) in the District of Columbia.

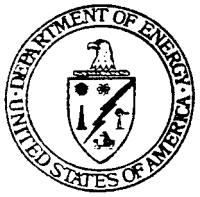
Sincerely,

William S. Maharay

William S. Maharay
Deputy Inspector General
for Audit Services
Office of Inspector General

Enclosures

Document Number 1



Department of Energy
Washington, DC 20585

Released

November 27, 2006

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Special Inquiry on "Selected Controls over Classified Information at the Los Alamos National Laboratory"

INTRODUCTION AND BACKGROUND

You asked that the Office of Inspector General examine the circumstances surrounding a recent incident at the National Nuclear Security Administration's Los Alamos National Laboratory concerning the possible compromise of classified data. Your request focused on what the Department of Energy and its contractors did or did not do to protect classified information, specifically, the steps that were taken to ensure that only properly qualified individuals had access to such information. This memorandum summarizes our findings in this matter. Because of cyber security and Privacy Act considerations, detailed findings are provided in a non-public attachment to this memorandum.

On October 17, 2006, Los Alamos County Police responded to a call at the home of a former employee of a Los Alamos National Laboratory subcontractor. During a subsequent search of that residence, police seized a computer flash drive that contained apparent images of classified documents from the Laboratory. Also found were several hundred pages of what appeared to be Laboratory documents with classified markings. The Federal Bureau of Investigation was notified and immediately began a separate review of this matter, which continues as of this date. Further, Laboratory and Departmental personnel have been involved in a number of related fact-gathering efforts. These matters have been widely publicized in local media.

Against this backdrop, the Office of Inspector General initiated a review to address the concerns raised in your letter. As part of this effort, we interviewed over 80 Departmental, Laboratory, and subcontract personnel; reviewed relevant security and cyber security guidance and procedures; and, examined numerous other documents.

OVERVIEW OF FINDINGS

We found that the security framework relating to this incident at Los Alamos was seriously flawed. Specifically, our review disclosed that:

1. In a number of key areas, security policy was non-existent, applied inconsistently, or not followed;
2. Critical cyber security internal controls and safeguards were not functioning as intended; and,
3. Monitoring by both Laboratory and Federal officials was inadequate.

ATTACHMENT TRANSMITTED CONTAINS
~~OFFICIAL USE ONLY~~

Cyber security has been an area of particular interest at Los Alamos due, in part, to well-publicized prior security incidents. In 1999, the then Secretary of Energy accepted a new plan for cyber security at Los Alamos – commonly referred to as the *Nine-Point Plan* – as a result of a high profile compromise of classified data. This plan specifically directed that safeguards be implemented to prevent the migration of classified information to unclassified systems. In a subsequent Secretarial initiative, called the *Six Further Enhancements to DOE Cyber Security*, both contractor and Federal officials were directed to take action to reduce the cyber security threat posed by insiders. In 2004, to address additional weaknesses in this area, the Director of the Laboratory ordered a lengthy, security stand-down to address and resolve such concerns. That shutdown, according to the U.S. Government Accountability Office, delayed important national security work at a significant monetary cost to the taxpayers. Based on the problems we observed, clearly these efforts were not entirely successful and additional improvements are needed.

The physical and intellectual data that resides at the Los Alamos National Laboratory reflects its preeminent national security mission. Yet, our review of matters related to the most recent incident identified a cyber security environment that was inadequate given the sensitivity of operations at the Laboratory. This was especially troubling since the Department and the National Nuclear Security Administration have expended tens of millions of dollars upgrading various components of the Laboratory's security apparatus, including vast expenditures on cyber security. In fact, the cyber security events described previously were among the factors that caused the Department to recompete the contract to operate Los Alamos. While significant procedural weaknesses were evident, human failure, whether willful or not, was the key component in this matter. In our report, we identified a number of specific actions associated with the latest series of events that were in contravention of recognized security policies and procedures.

Our detailed report also includes specific recommendations to strengthen security policy and procedures at both the Department and the Laboratory. On June 1, 2006, Los Alamos National Security LLC assumed responsibility as the operator of the Los Alamos National Laboratory. Many of these recommendations require specific contractor actions to address the weaknesses noted in our special inquiry. In this context, the Department needs to hold the new contractor accountable for the reforms needed to ensure a secure cyber security environment at Los Alamos. Further, we concluded that the lessons learned from this incident should be applied throughout the Department of Energy complex.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Chief of Staff

Document Number 2

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

Special Inquiry
Report to the Secretary

Selected Controls over Classified Information at the Los Alamos National Laboratory

OAS-SR-07-01 November 2006

SELECTED CONTROLS OVER CLASSIFIED INFORMATION AT THE LOS ALAMOS NATIONAL LABORATORY

SPECIAL INQUIRY ON SELECTED CONTROLS OVER CLASSIFIED INFORMATION AT THE LOS ALAMOS NATIONAL LABORATORY

TABLE OF CONTENTS

SELECTED CONTROLS OVER CLASSIFIED INFORMATION AT THE LOS ALAMOS NATIONAL LABORATORY

EXECUTIVE SUMMARY

b6, 7(C)

BACKGROUND

The Los Alamos National Laboratory (LANL) is operated by Los Alamos National Security, LLC for the Department of Energy's National Nuclear Security Administration (NNSA). Its more than 10,000 employees support various national security-related research and development activities. These efforts range from ensuring the safety and reliability of the Nation's nuclear stockpile and preventing the proliferation of weapons of mass destruction, to protecting the Nation from terrorist attacks. To support its mission, the Laboratory manages highly sensitive nuclear materials and classified information. Classified areas and processing facilities pervade much of the site, with over 2,700 separate classified operations, including 139 vault-type rooms. Safeguarding information and materials requires that the Laboratory establish and maintain effective security controls. Security, both physical and cyber, has been a long-standing concern at the Laboratory.

On October 17, 2006, evidence obtained during a drug-related investigation in the Los Alamos community revealed that classified information had been diverted from the Laboratory. Local law enforcement officers seized a flash drive containing classified data, as well as a large number of classified documents, [redacted] Because of the seriousness of these issues, and in response to a request by the Secretary of Energy, the Office of Inspector General initiated a review to determine whether the Department and the Los Alamos National Laboratory had adequately protected classified information in this instance and to examine the circumstances surrounding [redacted]

RESULTS OF REVIEW

Our review revealed a serious breakdown in core Laboratory security controls. In many cases, Laboratory management and staff did not enforce existing safeguards or they did not provide the attention or emphasis necessary to ensure a secure cyber environment. Some of the policies were conflicting and were applied inconsistently. In other cases, necessary controls had not been developed or implemented. We also found shortcomings in security policy formulation and monitoring activities by Federal officials. In short, these findings raised serious concerns about the Laboratory's ability to protect both classified and sensitive information systems.

We also noted that the NNSA failed to follow-up on issues relating to [redacted]

The diversion of classified material had a potentially serious impact on national security. As reported in various press accounts, [redacted]

Assuming there is no change in

While the control problems we identified were serious and created an environment in which the diversion could occur, the clear violations of security procedures appear to have been the root cause of the unauthorized removal of the classified material. These events are the subject of an on-going investigation by the Federal Bureau of Investigation, the results of which may ultimately provide additional information that should be considered in determining corrective actions. Not withstanding the investigative effort, our review found that a number of safeguards designed to protect classified information at LANL were not working as intended.

Classified Network and Computer Security Controls

The Los Alamos National Laboratory had developed policies designed to protect classified information. However, in many instances these policies and procedures were ineffective. For example:

- Ports that could have been used to inappropriately migrate information from classified computers to unclassified devices and computers had not been disabled. LANL management acknowledged that this vulnerability was not limited to the area in which but also existed in a number of other classified computing facilities;
- granted computer privileges that were not required
- Program and security officials permitted the introduction of computers and peripherals (scanners and a printer) into a classified computing environment even though they were not approved. Such devices could have been used to compromise network security.

These cyber security weaknesses resulted from control and management failures at multiple levels. In particular, we noted that policies designed to protect classified information were non-existent, not enforced or were inadequate. For example, the Los Alamos National Laboratory failed to:

- Enforce, in all cases, controls designed to prevent the migration of classified data to unclassified systems;
- Develop policies requiring system administrators to take advantage of readily available means to physically secure classified computers; and,
- Ensure that incompatible functions were segregated and that related compensating controls were in place and operating as intended.

We also found other weaknesses that limited the effectiveness of the Laboratory's classified information system protection program and may have contributed to the diversion of the classified information in this case. For example, Federal review of the Laboratory's classified

information systems was not as aggressive as it should have been. Also, we found that some of the Laboratory's policies for procuring classified information support services and for developing and administering system security plans were conflicting and inconsistent. Further, Federal policy design and implementation issues regarding mixed media vulnerabilities (mingling classified and unclassified computers and/or storage devices) were not adequately addressed and could have implications for the entire Department of Energy complex.

Security Clearance Process

[redacted]

On-Going and Needed Corrective Actions

After discovery of the incident, management officials at various levels of the Department and at LANL launched an effort to identify and correct control deficiencies that caused or contributed to the unauthorized removal of classified information. The Deputy Secretary issued a memorandum directing that each laboratory and Federal facility operating a classified computer system conduct an immediate and thorough examination of the adequacy of its practices and procedures to ensure that classified information is properly protected. LANL officials also reported that they had taken actions designed to increase the security over classified information, including securing open ports. Based on our preliminary review, we believe these steps could, if properly implemented, help resolve many of the problems we found. However, additional action is necessary. Consequently, we made a number of specific recommendations designed to: (i) increase the protection of classified information at LANL and other Departmental facilities; and, (ii) improve the integrity of the security clearance investigation and evaluation process.

DETAILED RESULTS OF REVIEW

b6, 7(C)

Introduction and Scope

During September 2005, LANL began a project to scan classified documents and create an electronic archive that could be searched by weapons developers and researchers. To accomplish this, the Laboratory tasked an existing subcontractor with providing some of the hardware needed for the project (scanners) and the labor to actually perform the scanning and indexing of the classified material. [ ] subcontractor's [ ] performed [ ] scanning and indexing of [ ]

[ ] The project [ ] one of the 95 separate archiving efforts in progress at LANL, [ ]

On October 17, 2006, the Los Alamos Police seized a flash drive containing classified information and a number of classified documents [ ] during a drug-related investigation. Subsequent analysis of the seized material revealed that it constituted a portion of the material involved in the scanning project and had been diverted from the Laboratory. Because of the seriousness of the diversion, the Secretary of Energy requested that the Office of Inspector General initiate a review to determine whether the Department and the Los Alamos National Laboratory had adequately protected classified information in this instance and to examine the circumstances surrounding [ ] In response to the request, we:

- Reviewed Department of Energy and Los Alamos National Laboratory policies and procedures governing cyber and physical security over classified information at the Laboratory;
- Examined the personnel security adjudicatio [ ]
- Interviewed over 80 federal and contractor officials;
- [ ]
- Conducted a physical observation of the VTR in question; and,
- Performed limited tests of general controls over classified information systems security at the Laboratory.

Classified Network and Computer Security Controls

Our examination disclosed that while the Los Alamos National Laboratory had developed policies designed to protect classified information, in many instances they were not effective in preventing serious security weaknesses. We identified deficiencies related to mixed media vulnerabilities, unneeded access to computing resources, as well as the failure to operate within classified information system accreditation boundaries.

b6,7C

Migration of Classified Information

Following a major security compromise in 1999, the then Secretary of Energy ordered LANL and other similarly situated facilities to implement controls and protections to make it physically impossible to migrate classified information to unclassified systems and devices. While LANL had taken action to disable a number of devices, in a significant number of instances, it did not deactivate open computer ports that could be used to circumvent such controls. [ ] none of the ports, in the classified rack-mounted computers that could be used to copy classified data, had been disabled or secured. Our review disclosed that [ ] open and unsecured USB and high speed serial (firewire) ports on the classified computers [ ] Such access would have permitted [ ] copying classified information to high capacity and easily concealable devices such as flash and portable hard drives. Information gathered by Laboratory line management officials immediately following [ ] flash drive further disclosed that [ ]

b2

Our examination also disclosed that mixed media weaknesses in the same VTR could have permitted the transfer of classified information to unclassified networks and/or systems. We found that at least one unclassified, standalone-computer had active and accessible USB and firewire ports and also had access to the Laboratory's yellow network – used for processing sensitive but unclassified information – and to the Internet. [ ]

b2

While forensic examination of all computers in the VTR had not been completed by the time we concluded our review, analysts told us [ ] classified information to the standalone unclassified computer's hard drive, transferred it LANL's unclassified network, or uploaded such information to the Internet. [ ]

Access to Resources

In spite of controls and specific guidance by NNSA to the contrary, [ ] granted access to a classified high-speed network printer even though not required [ ] Among other measures, the Laboratory developed safeguards designed to ensure that classified information and computer resources are adequately protected. For example, Information Systems Security Officers (ISSO) (and/or their alternates) are, among other responsibilities, required to ensure that user access is appropriate. In this case, however, that control was not effective. While the [ ] practice was to provide printer access to all users regardless of their duties. LANL contracting, program, and subcontractor officials we spoke with stated that [ ]

LANL officials confirmed through forensic analysis that [ ] the printer that was allegedly used for production of the hard-copy classified documents

b6, 7(c)

to physically access the classified computers contained in the VTR even though they were not authorized to perform systems administration tasks. As noted by the Laboratory's such practices endanger security and are specifically prohibited. Despite these risks, workers were permitted routine access to the unlocked racks to reset classified computers and various devices when needed. While the other duties and would not have known whether individuals continued to access the unlocked classified computer racks

Operating Within Accreditation Boundaries

LANL officials also permitted the subcontractor to introduce unapproved devices into the VTR even though they were not included in the accredited security plan and could have compromised the classified network. Although the sequence or timing of events could not be established with certainty, we confirmed that at some point during the scanning and archiving project that began in September 2005, the subcontractor responsible for the project introduced three of its own scanners into the VTR. While these items were called for in the subcontract task plan, they were not addressed in the system security plan and, as such, never received authority to operate from Federal accrediting officials. that while the particular scanner posed a security risk, - all actions specifically required by LANL policy.

In addition to the scanning devices, we also identified several unclassified computers and other peripherals that were present in the VTR but had not been included in its security plan. The most significant of these devices was the previously described classified high-speed printer to which That printer was capable of double-side printing – the format for many of the hard copy classified documents – and was connected to the Laboratory's classified network. Several other devices – an apparently unused (but still operational) unclassified computer and an additional government-owned scanner – were also present in the VTR, but had not been included on the latest security plan. As with the subcontractor-owned scanners, omission from the plan effectively prevented security officials from evaluating the impact of these peripherals. As a result, they were never reviewed by Laboratory classified computer security officials or approved for operation by Federal accrediting officials.

The accreditation issues we identified are parallel to problems that we identified during our annual *Evaluation Report on the Department's Unclassified Cyber Security Program – 2006* (DOE/OIG-0738, September 2006).

b5

b6, 7C

As noted in guidance published by the National Institute of Standards and Technology (NIST), accurate inventories are a key initial step in determining what system elements are exposed to security risks.

Structural Control and Implementation Weaknesses

These cyber security weaknesses resulted from control and management failures at multiple levels. In particular, we noted that policies designed to protect classified information were not enforced or were inadequate. For example, the Los Alamos National Laboratory had not:

- Taken adequate action, in all cases, to enforce controls designed to prevent the migration of classified data to unclassified systems;
- Developed policy requiring system administrators to take advantage of readily available means to physically secure classified computers; and,
- Ensured that incompatible functions were segregated and related compensating controls were in place and operational.

Migration Vulnerabilities

Although LANL had developed policies designed to prevent the unauthorized transfer of classified information to unclassified media or devices, the policies and procedures were not properly implemented and were not always effective. [ ] classified network operations and various members of [ ] recognized that open ports in mixed media environments posed a risk and that they "should have paid better attention" to ensuring that policies designed to prevent migration of classified systems were enforced. [ ] that in many situations – such as in [ ] – action had been taken to secure ports by covering them with tamper-indicating tape and, in some other environments, ports had been disabled through software controls. In response to our inquiry, [ ]

b2

While network engineering officials and others within the LANL Chief Information Officer's organization expressed concerns with open ports and problems with managing tamper-indicating devices, a Laboratory-wide solution was never developed or deployed. As evidenced by a series of e-mail exchanges between members of a "diskless computer discussion group" during the March-April 2006 timeframe (with copies provided to the NNSA's Los Alamos Site Office), group members responsible for configuring computers were concerned that a common technical solution to "address the control of USB/Firewire ports" in mixed media environments had not been developed. In discussing the security challenges associated with modern, multi-port computers, one member of the group recognized that it "would be a simple matter to plug some recording device into one of these open ports and write to it."

LANL management officials acknowledged, during security briefings related to the discovery of the diversion of classified information, that the actions to disable USB ports in mixed media environments had not been completely effective in the past. They noted that after the recent diversion of classified information they had identified a number of environments where ports

remained accessible. As part of its remediation effort initiated after the current problem was discovered, Laboratory management reported that it had required each user to re-review classified information security requirements, had secured virtually all vulnerable USB ports, and had directed that all flash drives be collected and controlled. We were unable to verify in the available timeframe that the actions described by management had actually been completed.

Security of Rack-Mounted Computers

LANL also failed to take advantage of readily available security measures that, in this case, would most likely have prevented the unauthorized removal of the electronic classified material found on the seized flash drive. A senior laboratory management official told us that as part of its initiative to secure CREM following a major security event in 2002, they had acquired locking racks that were to be used to secure most rack-mounted classified computer systems. Although uncertain of the timing, that official explained that at some point the decision was made that these rack mounted systems did not contain CREM and that there was no need to secure them if they were located in vaults or VTRs. Both computer security and management officials that we consulted at the Laboratory informed us that securing these racks would have denied access to the enabled USB ports in the VTR in question and that such action could have prevented the download of the diverted classified information (See Appendix 2). After discussing this issue with Laboratory management officials, these officials indicated that they have now directed that all classified computer racks be locked regardless of their location.

Segregation of Incompatible Functions

The assignment of incompatible functions by LANL to a single individual might have contributed to the unauthorized removal of classified information in this case. As specified by NNSA policy, "...measures must be implemented to ensure the management, control, and separation of security critical functions." In this case, however, LANL did not always provide for such separation, and provided a single individual with unfettered authority to override safeguards designed to protect classified systems. For example, [ ] granted physical access to classified computers to unauthorized individuals, including [ ] also provided with the same authority and overrode controls designed to prevent peripherals that were not owned by the government and/or had not been evaluated for security impacts from being introduced into the classified computing environment. Essentially, these individuals were given the authority to supervise and approve their own actions. The [ ] were particularly important in this case because these actions may have desensitized [ ] in and around the classified computer racks – a situation that could have permitted [ ] insertion and removal of the flash drive from the classified computer without detection.

Because of the extent to which ISSOs are assigned as system administrators in other organizations, the same or similar problems may exist at a number of other LANL facilities. When initially queried, the Laboratory's [ ] could not easily determine how many individuals were serving in dual-role capacities. [ ] that line managers selected and appointed the ISSOs, that ISSOs were authorized to appoint alternates in

b6, 7(C)

some areas, and that the only way [ ] quantify the incompatible assignment issue was to put out a data call. Although the data collection effort had not been concluded at the time our field work was completed, we did learn that, with about 80 percent of organizations reporting, 62 percent of the individuals identified could be in the position of supervising their own work.

While the Laboratory's [ ] aware of the benefits of segregation of duties in preventing or detecting security problems involving insiders, [ ] not believe that regulations required such separation and stated that funding was insufficient to accommodate it. [ ] that the Laboratory interpreted the Department's *Classified Information Systems Security Manual* (DOE M 471.2-2 of August 3, 1999) as not requiring that the ISSO and the system administrator functions be separated for protection levels such as those employed at LANL. We found, however, that the cited manual is inconsistent with current NNSA guidance. The Department's Manual also does not comport with guidance established by the NIST and the Office of Management and Budget (OMB) that stress the need for separation of incompatible functions, and, when such separation is not practical, the requirement to employ strong compensating controls.

Compensating Controls

While the Laboratory developed a mechanism designed to help ensure that the actions of those who administer classified information systems were appropriate, it was not effective and potentially contributed to the unauthorized removal of classified material. Every [ ] is charged with the responsibility of ensuring that actions of their alternates are appropriate and consistent with existing policy. After detailing the management and review role expected of those in [ ] unable to properly fulfill [ ] workload was just too large [ ] was forced to delegate virtually all [ ] functions [ ] inexperienced in the requirements of administering and securing classified networks. [ ] visit [ ] infrequently; [ ] unaware of the scanning project; did not perform testing or reviews of controls [ ] had not detected any of the particular control overrides we identified.

LANL management indicated that it tried to compensate for segregation of duty problems by requiring the participation of others in the testing of security plans. Computer security officials indicated that other system administrators, often from different organizations, participated in testing security plans to determine their viability. While they conceded that the same individual that prepared the plans was sometimes responsible for testing, they also stated that from two to five separate individuals experienced in systems administration were often involved in testing. In this instance, however, the compensating control was not effective in that the other testers involved in a June 2006 test did not identify mixed media vulnerabilities, problems associated with the omission of peripherals from the security plan, or the introduction of subcontractor-owned and other equipment. LANL relied completely on this compensating control and did not require its [ ] to visit locations to verify that both plans and testing were appropriate.

Contributing Factors

We also found other weaknesses that, in our opinion, limited the effectiveness of the Laboratory's classified information system protection program and contributed to the unauthorized diversion of classified information in this case. These included inadequate Federal review and inspection of the Laboratory's classified information systems; conflicting and inconsistent policy for procuring classified information support services and for adequately maintaining system security plans; and, Federal policy design and implementation issues that could have implications for the entire Department of Energy complex.

Federal Management and Review Activities

The failure of Federal security officials to perform verification activities may have adversely affected the classified security climate at the Laboratory and contributed to the recent removal of classified material. The Los Alamos Site Office (LASO) performed a number of management activities; however, it did not complete needed field activity reviews of the Laboratory's classified information systems. Accrediting officials at LASO told us that they placed a great deal of emphasis on reviewing security plans and accrediting systems, but because of resource constraints, they were unable to perform physical inspection of systems to validate that the plans were accurate and were being enforced.

During Fiscal Years 2005 and 2006, LASO officials reported that they had only 1.5 full time equivalents available for review of contractor systems and that they simply did not have time to visit system locations. Our current observations at LASO are consistent with findings we issued in connection with our *Evaluation Report on the Department's Unclassified Cyber Security Program – 2006* (DOE/IG-0738, September 2006), in which we expressed our view that NNSA site offices did not adequately manage cyber security by ensuring that contractors implemented NIST and OMB cyber security requirements. In response to our 2006 finding, NNSA indicated that it did not concur with our view and noted that existing mechanisms were sufficient to meet requirements. Following the incident under review, LASO officials told us that they had reevaluated resource allocations in this area and planned to begin a series of field activity reviews in the near future.

Problems with the timely completion of classified information system inspections may have also been a factor in conditions we identified. Except for an annual review conducted by a senior cyber security specialist from its Service Center, NNSA relied on the Office of Independent Oversight, Office of Health, Safety and Security to conduct detailed reviews of LANL's classified information systems. Although normally completed once every two years, this inspection had not been performed for about four years because of a variety of factors. Office of Independent Oversight officials told us that a significant portion of the delay was caused by the security stand down at LANL in 2004, a moratorium placed on reviews during the period that the contract was transitioned from the University of California to Los Alamos National Security, LLC (LANS), and, finally, their participation in a number of Site-Assisted Visits as part of the Department's Cyber Security Revitalization Plan. It should be noted that the Office of Independent Oversight began a previously scheduled review of LANL's classified information systems at about the same time the diversion of classified information was discovered.

b6, 7(C)

Security Planning and Acquisition Policy Issues

We found conflicting direction regarding what items to include in security plans, a factor that may have impacted cyber security at LANL. For example, the Laboratory's [ ] from the NNSA Service Center had directed that peripheral devices not be included in security plans. Based on that direction, [ ] ISSOs to only include peripherals if their cost was equal to or more than the property accountability threshold for the Laboratory. In contrast, LANL's [ ] us that all peripherals except for small items that had no memory or ability to read or write information – items such as a mouse or keyboard – were to be included, and their impact evaluated, in security plans. [ ] had "heard something about" the direction regarding peripherals but had not verified the direction or evaluated its impact. The NNSA Service Center [ ] told us that [ ] not provided such guidance.

A lack of knowledge of policy regarding the introduction of equipment following completion of security plans could also have impacted classified information systems security at some of the 104 similarly situated VTRs located across LANL. As identified in LANL guidance, ISSOs are required to update security plans and seek reaccreditation whenever significant changes to the configuration of a system occurred. When queried as to why the security plan for the [ ] was not updated when new devices or systems were introduced, the [ ] told us that the Laboratory has no specific policy regarding events that could trigger the requirement to update security plans. [ ] on individual ISSOs to make their own determination as to what is significant and whether an update was required, and, as we noted earlier, it was not [ ] We observed that the Laboratory had issued policy in August 2002, which specifically described events that would trigger a change to security – several of which appeared to be directly applicable in this case.

b2

Inconsistent and conflicting policy regarding the acquisition of computer support services also impacted security in classified computing environments at the Laboratory. For the task under which the classified scanning took place (as well as for a number of others), procurement officials required that the subcontractor furnish peripherals such as scanners and software. This requirement was incorporated into the task even though the NNSA Policy Letter (NAPS) governing classified computer security and the local classified system security plan for the VTR in question specifically prohibited the connection of non-government owned equipment to the classified local area network. Several months before our review, LANL issued a policy inconsistent with the NAPS in that it permitted the use of non-government property if it was properly reviewed and sanitized upon removal.

Federal Policy Design Issues

Our review disclosed at least one particularly significant instance where classified computer policies had not been developed or properly formalized. After a major breach involving the removal of classified material from LANL in 1999, the then Secretary of Energy directed that

safeguards be developed and implemented to prevent the migration of classified data to unclassified systems and decrease the potential for insiders to exploit security vulnerabilities. This direction specifically required that organizations "establish requirements that place stringent controls on computers and work stations, including controls on ... ports that could be used to download files." While ordered and implemented for the three laboratories under the cognizance of the then Albuquerque Operations Office, the requirement was never included in the Department's or the NNSA's cyber security policy. Despite efforts by the Department's Chief Information Officer and various working groups chartered by that organization, this and other policies related to national security systems, including many of those required by the Federal Information Systems Security Management Act (FISMA), have yet to be incorporated in Department policy.

A senior official with the Office of Independent Oversight indicated that [ ] organization had reported on the Department's failure to update its classified computer security policy. As noted in its *Report on the Status of the Department of Energy's Information Security Program for National Security Systems* (September 2006), issued to satisfy FISMA evaluation requirements, the Office of Independent Oversight reported that policies for protecting national security systems had not been updated since 1999 and were seriously out of date. The inspectors concluded that policy weaknesses contributed to a number of FISMA implementation vulnerabilities that could, if not corrected, endanger classified systems. Most notably, [ ] b2

Cyber Security Program Implementation Issues

Laboratory officials, including the [ ] informed us that they were committed to providing a multilayered defense against both internal and external parties that may wish to damage computer systems or compromise information. While these officials indicated that they have recently strengthened their resolve to achieve this goal in response to the recent diversion of classified information, they identified what they believed to be significant structural issues that have frustrated their efforts in this regard. Specifically, during the transition of the operating contract from the University of California in mid-2006, LANS identified cyber security as a preexisting condition, [ ] b2

The preexisting condition related to cyber security, one of several identified during the contract transition phase, was based primarily on the fact that the University of California had not implemented most of the NNSA cyber security implementing guidance. The Laboratory's [ ] b2

[ ] as specified in the NAPS, and provided information that indicated that only a small fraction of those requirements had been implemented to date. In addition to the preexisting condition identified prior to contract transition, LANL also told us [ ] On b2

September 27, 2006, [ ] concern that [ ] b2

b6, 7(C)

NNSA's [redacted] for cyber security at the national defense laboratories.

Ongoing Reviews and Corrective Actions

Management officials at various levels of the Department and at LANL promptly launched an effort to identify and correct control deficiencies that caused or contributed to the unauthorized removal of classified information. The Deputy Secretary also issued a memorandum directing that each laboratory and Federal facility operating a classified computer system conduct an immediate and thorough examination of the adequacy of its practices and procedures to ensure that classified information is properly protected. LANL officials also reported that they had taken actions designed to secure open ports and increase security over classified information. To facilitate this work and provide technical assistance, the Department's Chief Information Officer told us that his office had commissioned a study to identify and evaluate the relative strengths and weaknesses of the various hardware and software methods of securing computer ports and is working to update classified cyber security policy.

National Security Impacts

The seriousness of the theft or diversion of classified material could have a significant impact on U.S. national security. If exploited, such information could be used to damage critical facilities and disrupt Government operations. For this event in particular, the full extent of damage or dispersion of the classified material removed by the alleged perpetrator may never be fully known. [redacted]

b7

RECOMMENDATIONS

Although a number of cyber security initiatives are underway, we concluded that the Department needs to reemphasize its commitment to cyber security. In addition, to address the weaknesses described in our report, we recommend that the Under Secretary for Nuclear Security/Administrator of National Nuclear Security Administration, working with the Chief Information Officer and the Chief Health, Safety and Security Officer, complete the following detailed actions, all of which may have applicability across the complex:

1. Ensure that classified cyber security policies and implementing instructions are updated to address noted deficiencies;

2. Disable unneeded active USB and other system ports that could permit the unauthorized diversion or theft of classified information;

3. Secure classified computer racks;

4. Ensure that incompatible duties (supervision and actual performance of tasks) are not performed by the same individual;

5. Limit classified computer access and privileges to those who specifically require it;

6. Require that classified information security plans be complete and accurate, be updated for changes, and that accreditations are obtained prior to operation;

7. Conduct both contractor and Federal reviews and physical inspections of systems prior to granting authority to operate, and periodically throughout the accreditation period;

8. Reevaluate cyber security funding, using a risk-based approach; and,

9. Review activities by Federal and contractor management and staff to determine whether administrative action is appropriate.

To further reduce risks at LANL and other Department facilities, we recommend that the Under Secretary for Nuclear Security/Administrator, National Nuclear Security Administration:

10. Monitor on-going classified cyber security efforts to ensure that all needed corrective actions are tracked to resolution;

11. Share the lessons learned in this case with each of the Department's facilities; and,

12. Coordinate with the Chief Health, Safety and Security Officer, Office of Independent Oversight to ensure that a follow-up inspection to validate the efficacy of each corrective action and the overall viability of LANL's classified cyber security protection program is performed. In addition, evaluate inspection protocols to ensure that the vulnerabilities cited in this report are tested periodically.

On June 1, 2006, Los Alamos National Security LLC assumed responsibility as the operator of the Los Alamos National Laboratory. Many of the recommendations, noted above, require specific contractor actions to address the weaknesses noted in this report. In this context, the Department needs to hold the new contractor accountable for the reforms needed to ensure a secure cyber security environment at Los Alamos.

b6,7(c)

Security Clearance Process

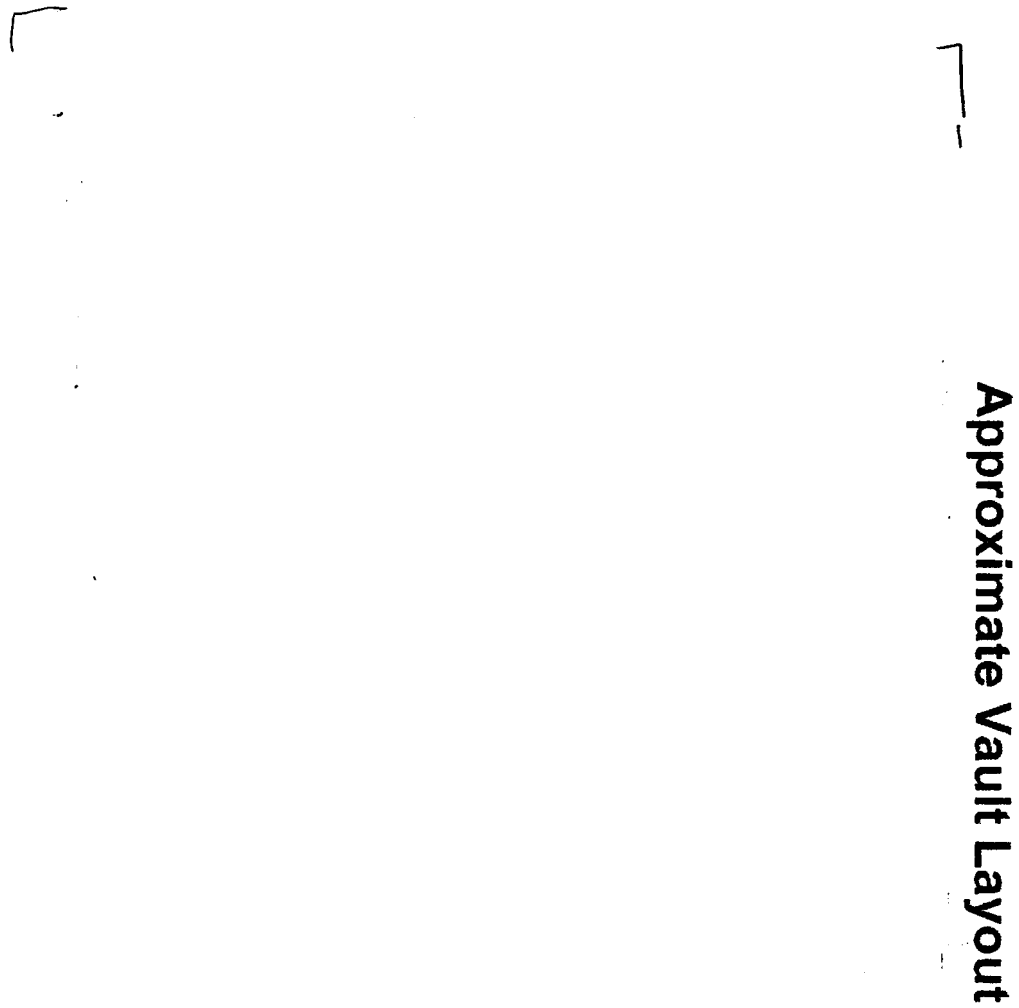
[ ] b6, 7(C)

RECOMMENDATIONS

APPENDIX 1

b2

DIAGRAM OF VAULT-TYPE ROOM



APPENDIX 2

b2

RELATED PHOTOGRAPHS

APPENDIX 3

PRIOR REPORTS

- *Audit Report on the Department of Energy's Fiscal Year 2006 Consolidated Financial Statements* (OAS-FS-07-02, November 2006). Vulnerabilities and weaknesses continued to exist in the Department's network and information systems for access and other security controls. Specifically, the National Nuclear Security Administration (NNSA) failed to ensure that Federal, Departmental, and NNSA cyber security requirements, policies, and controls were always properly implemented by field organizations and facilities contractors. Program officials had not ensured that facility operating contracts were modified to incorporate all Federal cyber security requirements. Further, many systems' certifications and accreditations (C&A) had not been performed, lacked essential elements such as independent testing of the effectiveness of security controls, or were not adequately documented. In addition, certain sites incorrectly used an overly broad grouping or "enclave" approach to completing the C&A of their systems. Vulnerabilities and weaknesses continued to exist in access and other security controls, which increased the risk that malicious destruction, alteration of data, or unauthorized processing could occur.

- *Evaluation Report on the Department's Unclassified Cyber Security Program - 2006* (DOE/IG-0738, September 2006). The evaluation identified continued deficiencies in the Department's cyber security program that exposed its critical systems to an increased risk of compromise. The report cited weaknesses in the following areas: systems inventory, system certifications and accreditations, contingency planning, physical and logical access controls, configuration management, and change controls. Problems occurred, at least in part, because Departmental organizations had not always ensured that Federal requirements, Department policies, and cyber security controls were adequately implemented and conformed to Federal requirements, most notably by field organizations and facility contractors. NNSA site officials indicated that they were required to comply with NNSA cyber security policy, as opposed to meeting NIST requirements. Accordingly, no NNSA site had fully implemented the NNSA cyber security policy. In fact, many NNSA field sites were permitted to follow a less thorough certification and accreditation process that did not incorporate all NIST or NNSA requirements. As a result, the Department's information systems, networks, and the information they contain remain at risk of compromise.

- *Special Inquiry Report Relating to the Department of Energy's Response to a Compromise of Personnel Data* (OIG Case No. I06IG001, July 2006). The inquiry found that a hacker had exfiltrated a file containing the names and social security numbers of 1,502 Federal and contractor employees working at NNSA's Service Center in Albuquerque, New Mexico. Neither the employees affected nor appropriate officials were properly notified about the compromise until about ten months after the successful intrusion had been detected. In addition, there was a lengthy delay in the Department's completion of an impact assessment on the intrusion. The Department's handling of this matter was largely dysfunctional and the operational and procedural breakdowns were caused by questionable managerial judgments; significant confusion by key decision makers as to lines of authority, responsibility, and

accountability; poor internal communications, including a lack of coordination and a failure to share essential information among key officials; and, insufficient follow-up on critically important issues and decisions. Additionally, the Department lacked clear guidance on procedures for notifying employees when personnel data is compromised. The bifurcated organizational structure of NNSA within the Department complicated the situation.

- *Inspection Report on Badge Retrieval and Security Clearance Termination at Sandia National Laboratory – New Mexico* (DOE/IG-0724, April 2006). Sandia National Laboratory's internal controls were not adequate to ensure that, in accordance with applicable policies and procedures, security badges assigned to terminating Sandia and subcontractor employees were retrieved at the time of departure or that security clearances of terminating Sandia and subcontractor employees were terminated in a timely manner. Specifically, from the same sample of 182 employees, 47 did not have complete Security Termination Statements, as required. Thus, there was no assurance these individuals had received the required Security Termination Briefing at the time of their termination. Given the similarity of the findings at the three National Laboratories reviewed, senior Department management should consider taking broader action within the Department to ensure that all Department sites are adequately addressing the areas of badge retrieval and security clearance termination. These areas are critical to the Department's program to control access to sensitive and classified information and facilities.

- *Audit Report on the Department of Energy's Fiscal Year 2005 Consolidated Financial Statements* (OAS-FS-06-01, November 2005). Network and information system security weaknesses continue to be identified at sites and the frequency and severity of those weaknesses remained consistent with prior year findings. The Department recognizes these weaknesses and has classified cyber security as a significant issue in its *Federal Managers' Financial Integrity Act* assurance statement for fiscal year 2005. Significant improvements are still needed in the areas of password management, configuration management, and restriction of network services. These findings remain open as of the issuance of the *Audit Report on the Department of Energy's Fiscal Year 2006 Consolidated Financial Statements* (OAS-FS-07-02, November 2006).

- *Inspection Report on Security and Other Issues Related to Out-Processing of Employees at Los Alamos National Laboratory* (DOE/IG-0677, February 2005). The Los Alamos National Laboratory (LANL) directly employed about 7,500 University of California employees, of which approximately 800 terminate their employment each year. LANL out-processing procedures were not followed by more than 40 percent of the 305 terminating employees included in the selected sample during the period under review. Consequently, Property Administrators, Classified Document Custodians, and Badge Office personnel frequently did not receive timely notification that employees were terminating. Given this and the results of additional sampling, there was no assurance that, prior to departure, LANL terminating employees turned in security badges, completed the required Security Termination Statement, or had their security clearances and access authorizations to classified matter and/or special nuclear material terminated in a timely manner.

- *Inspection Report on Internal Controls over Personal Computers at Los Alamos National Laboratory*, (DOE/IG-0656, August 2004). An interim inspection report (DOE/IG-0597, April 2003) on the same subject documented internal control weaknesses regarding LANL computers, particularly classified and unclassified laptop computers, including accountability and accreditation issues. This follow-on report identified continuing internal control weaknesses that undermined confidence in LANL's ability to assure that (1) computers are appropriately controlled and safeguarded from loss or theft and (2) computers used to process and store classified information are controlled in accordance with existing property management and security requirements. Specifically, a number of classified desktop computers were not entered into the LANL property inventory, as required, and some were not assigned a property number. In addition, LANL's listing of classified desktop and laptop computers was not completely accurate, and computer identification in accreditation paperwork did not always match the actual classified equipment.

- *Inspection Report on Internal Controls Over Classified Computers and Classified Removable Media at the Lawrence Livermore National Laboratory* (DOE/IG-0628, December 2003). Certain internal control weaknesses were identified in Livermore's administration of its classified computer and classified removable media inventories, increasing the vulnerability of these items to loss, abuse, and theft. Specifically, Classified Nuclear Emergency Search Team computer equipment and removable media were not subjected to required inventories; six classified desktop computers that had been shipped permanently to other Department sites remained in Livermore's property inventory; and a classified removable hard drive was not entered into Livermore's classified removable media tracking and accounting system, as required. Given current national security concerns, the Department and its contractors should make a maximum effort to safeguard classified computers and classified media to reduce the possibility of loss, abuse, and theft.

- *Special Inquiry on Operations at Los Alamos National Laboratory* (DOE/IG-0584, January 2003). The OIG conducted a fact finding inquiry into the allegations that senior management of LANL engaged in a deliberate cover-up of security breaches and illegal activities, in particular, with respect to reported instances of property loss and theft. The report 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. These actions created an atmosphere in which Los Alamos employees were discouraged from, or had reason to believe they were discouraged from, raising concerns to appropriate authorities. In short, management's actions - whether intended as a cover-up or not – resulted in delayed identification and resolution of the underlying property and procurement weaknesses, and related security concerns. Although our inquiry did not substantiate the allegation that Laboratory management deliberately hid criminal activity, we found that Laboratory management failed to take appropriate or timely action with respect to a number of identified property control weaknesses, and related security concerns. Specifically, there was a lack of personal accountability for property and inadequate controls over procurement and property systems.

Prior Independent Oversight Reports

- Independent Oversight Report on the *Status of the Department of Energy's Information Security Program for National Security Systems*, September 2006

- Independent Oversight *Cyber Security Inspection of the Los Alamos Site Office and Los Alamos National Laboratory, Volume II*, January 2003

Prior Government Accountability Office (GAO) Reports

- *Stand-Down of Los Alamos National Laboratory: Total Costs Uncertain; Almost All Mission-Critical Programs Were Affected but Have Recovered* (GAO-06-83, November 2005). On July 16, 2004, the Director of LANL suspended all activities except those specifically designated as critical, citing a pattern of safety and security incidents that occurred over the course of a year. Specifically, in the weeks prior to the stand-down, an undergraduate student was partially blinded in a laser accident, and two classified computer disks were reported missing. In both cases, laboratory employees disregarded established procedures and then attempted to cover up the incident. On July 23, 2004, the Deputy Secretary of Energy ordered a Department-wide stand-down of operations that used accountable classified removable electronic media. These media include computer disks; removable hard drives; and compact discs, read-only memory (CD ROM) that contain information classified as secret restricted data, top secret, or specially sensitive information. Almost all Department facilities resumed operations within 6 weeks, once they had certified that these media were accounted for and posed no security risk. Neither LANL's $121 million estimate nor NNSA's $370 million estimate, which it considers an upper bound, accurately captures the total cost of the LANL stand-down. LANL did not establish separate stand-down activity codes to track the actual time spent on stand-down activities, such as safety reviews and training. As a result, neither NNSA nor GAO can calculate actual stand-down costs.
- *Nuclear Security: Lessons to Be Learned from Implementing NNSA's Security Enhancements* (GAO-02-358, March 2002). Several security incidents in the late 1990s highlighted the need for improvements at the Department of Energy. For example, the possible loss of nuclear weapons design information and the "missing" computer hard drives at LANL revealed important weaknesses in security. More broadly, many reports have criticized Departmental security: the President's Foreign Intelligence Advisory Board report, the Cox Committee report, and a number of other GAO reports on particular aspects of the Department's security program. In response to individual events and reports, the Department, and later NNSA, developed initiatives intended to address nuclear security problems. Numerous initiatives were undertaken to strengthen, among other things, personnel, physical, information, and cyber security as well as the Department's counterintelligence program. Successful implementation of the initiatives should reduce the likelihood of security problems and therefore enhance security at NNSA facilities. For example, the Department has eliminated the backlog of security clearance investigations and reinvestigations of employees with access to classified information. Eliminating this backlog ensures that those employees with access to classified information have had their backgrounds checked and that cleared personnel needed in important mission-related areas are available for work. Other initiatives can strengthen controls over cyber security. The Department had published 29 cyber security directives for classified and unclassified systems and had provided cyber

security training for system administrators and managers. However, initiatives should be clearly communicated to the field. Contractor officials at one national laboratory received guidance on some cyber security initiatives from multiple offices within the Department and NNSA, often through informal means such as web site postings or verbal communication. This lack of clear communication produced confusion at sites about which requirements they needed to implement.

- *Nuclear Security: DOE Needs to Improve Control Over Classified Information (*GAO-01-806, August 24, 2001*).* The Los Alamos and Sandia National Laboratories have implemented Department of Energy's access controls and need-to-know requirements for both vaults and classified computer systems containing the most sensitive classified information. However, the Department's requirements for documenting need to know lack specificity, allowing laboratory managers wide variation in interpretation and implementation. Need-to-know determinations made by laboratory managers vary from detailed, specific, individual justifications to long-term blanket approvals for hundreds of staff for all classified information in a vault or computer system. More specific requirements and guidance for documenting need-to-know determinations would help ensure that only persons who require access to specific classified information to conduct their current work are granted access to that information. The Department had taken steps to upgrade protection and control over its classified information, but additional steps are needed. The Department's recent revision of its Classified Matter Protection and Control Manual adds several security requirements for top secret information. However, the revised manual does not reinstitute several top secret security requirements, in effect prior to 1998, that would enhance the protection of top secret information by providing a more traceable record of the document if it were to be lost. In addition, the Department was revising its Control of Weapon Data order to increase the security of documents that contain compilations of highly sensitive nuclear weapons information. This effort to upgrade security for the most sensitive weapons documents has already been under way for almost eight years. Until the order is issued and implemented, these documents will have a lower degree of protection.

- *Department of Energy: Key Factors Underlying Security Problems at DOE Facilities (*GAO/T-RCED 99-159, April 1999*).* The report disclosed security-related problems with controlling foreign visitors, protecting classified and sensitive information, maintaining physical security over facilities and property, ensuring the trustworthiness of employees, and accounting for nuclear materials. Among others, problems included 1) weaknesses in efforts to control and protect classified and sensitive information where one instance a facility could not account for 10,000 classified documents. 2) Lax physical security controls, such as security personnel and fences, to protect facilities and property. Our reviews of security personnel have shown that these personnel have been unable to demonstrate basic skills such as arresting intruders or shooting accurately; at one facility, 78 percent of the security personnel failed a test of required skills. Furthermore, GAO found that equipment and property worth millions of dollars was missing at some facilities. 3) Ineffective management of personnel security clearance programs has been a problem since the early 1980s. Backlogs were occurring in conducting security investigations, and later, when the backlogs were reduced, and some contractors were not verifying information on prospective employees.