Summary of Statement by Gregory H. Friedman, Inspector General

Secretary Bodman requested that the Office of Inspector General begin a review of the possible compromise of classified information at the Los Alamos National Laboratory.

Our special inquiry disclosed that computer ports, which could have been used to inappropriately migrate information from classified systems to unclassified devices and computers, had not been disabled; classified computer racks were not locked; individuals were inappropriately granted access to classified computers and equipment; computers and peripherals that could have been used to compromise network security were introduced into a classified computing environment without approval; and, critical security functions had not been adequately segregated.

In many instances, Laboratory management and staff had not developed policies necessary to protect classified information. Further, Laboratory and Federal officials were not as aggressive as they should have been in conducting security reviews and inspections. Our findings raised serious concerns about the Laboratory's ability to protect both classified and sensitive information systems.

We provided the Department with a number of specific recommendations designed to assist it in its efforts to correct identified deficiencies. In addition, at the request of the Subcommittee, we identified several broader actions that could improve the overall security climate at Los Alamos.

Statement of Gregory H. Friedman

Inspector General

U.S. Department of Energy

Before the

Subcommittee on Oversight and Investigations

Committee on Energy and Commerce

U.S. House of Representatives

FOR RELEASE ON DELIVERY
10:00 AM
Tuesday, January 30, 2007

Mr. Chairman and members of the Subcommittee, I am pleased to be here at your request to testify on the Office of Inspector General's review of the recent compromise of classified data at the Department of Energy's Los Alamos National Laboratory.

BACKGROUND

The Los Alamos National Laboratory, now operated by Los Alamos National Security, LLC, for the Department's National Nuclear Security Administration (NNSA), has been at the forefront of our country's national security-related research and development enterprise for over 60 years. The physical and intellectual data that resides at the Laboratory reflects its critically important missions, which range from ensuring the safety and reliability of our nuclear stockpile and preventing the proliferation of weapons of mass destruction to protecting the Nation from terrorist attacks. To support these missions, the Laboratory manages highly sensitive classified materials and information. Safeguarding such classified information – housed at over 2,700 separate classified computing operations, including 139 vault-type rooms – requires that the Laboratory establish and maintain strong security controls.

Over the years, there have been a number of highly-publicized security incidents that have cast doubt on the Los Alamos National Laboratory's ability to protect classified national security assets. In 1999, a Los Alamos scientist was accused of and subsequently pled guilty to mishandling classified information by downloading nuclear secrets and removing them from the Laboratory. In the following year, largely in response to security concerns at Los Alamos, the NNSA was established as a semi-autonomous agency. In 2002, two computer

hard drives containing classified data were thought to be missing from a secure area within the Laboratory, but were later found. In 2004, after an inventory indicated that two computer disks containing classified information were missing, the Director of the Laboratory ordered a lengthy stand-down to address and resolve security concerns. That stand-down, according to the U.S. Government Accountability Office, delayed important national security work at a substantial cost to the taxpayer.

Because of the need to ensure that the Nation's vital nuclear material and information are adequately protected, the Office of Inspector General has performed numerous audits, inspections, and investigations of physical and cyber security-related issues at the Laboratory. Our reviews have covered diverse areas such as the implementation of the design basis threat, safeguards over classified material and property, and the security of information systems. I have been asked to testify before this Subcommittee and other Congressional panels on several occasions regarding a series of management and security issues at Los Alamos.

As has been well-publicized, on October 17, 2006, the Los Alamos County Police Department responded to a call at the home of a former employee of a Laboratory subcontractor. During a subsequent search of the residence, police seized a computer flash drive that contained electronic images of Los Alamos classified documents. In addition, hard copies of over 200 classified documents belonging to the Laboratory were also found in the residence. Laboratory officials determined that the seized classified information was derived from an ongoing scanning and archiving project. This scanning project was being performed by a subcontractor to the Laboratory. A criminal investigation regarding the seized material was

initiated by the Federal Bureau of Investigation. Shortly after the investigation began, the Secretary of Energy requested that the Office of Inspector General perform a separate review of the possible compromise of classified information at the Los Alamos National Laboratory. The Secretary also asked that we evaluate certain aspects of the Department's security clearance process.

OFFICE OF INSPECTOR GENERAL REVIEW

The Office of Inspector General promptly began a special inquiry that focused on what the Department and its contractors did or did not do to protect classified information and the steps that were taken to ensure that only properly qualified individuals had access to such information. As part of that effort, we interviewed over 80 Departmental, Laboratory, and subcontractor personnel; reviewed relevant security guidance and procedures; and, examined numerous other relevant documents. Our findings related to the security clearance process should be discussed in closed session.

Our special inquiry revealed that despite the expenditure of millions of dollars by the NNSA to upgrade various components of the Laboratory's security apparatus, the security environment at the Laboratory was inadequate.

In particular we found that:

- Certain computer ports, which could have been used to inappropriately migrate information from classified systems to unclassified devices and computers, had not been disabled;
- Classified computer racks were not locked;
- Certain individuals were inappropriately granted access to classified computers and equipment to which they were not entitled;
- Computers and peripherals (scanners and a printer) that could have been used to compromise network security were introduced into a classified computing environment without approval; and,
- Critical security functions had not been adequately separated, essentially permitting system administrators to supervise themselves and override controls.

In many cases, Laboratory management and staff had not developed policies necessary to protect classified information, had not enforced existing safeguards, or provided the attention or emphasis necessary to ensure protective measures were adequate. Some of the security policies were conflicting or applied inconsistently. We also found that Laboratory and Federal officials were not as aggressive as they should have been in conducting security reviews and physical inspections. In short, our findings raised serious concerns about the Laboratory's ability to protect both classified and sensitive information systems.

Any diversion of classified material creates a potentially serious national security situation. For this event in particular, the full extent of damage or dispersion of the classified material

may never be fully known. The criminal investigation into this matter is ongoing and may yet reveal additional security problems. Our findings, however, which are discussed in more detail in the following paragraphs, underscore continuing problems with the Laboratory's overall management and security posture.

Open Computer Ports

Following the security incident in 1999, the then Secretary of Energy ordered the Los Alamos National Laboratory and other similarly situated facilities to implement controls and protections to make it physically impossible to migrate classified information to unclassified systems or devices. Although Los Alamos had taken action to disable some devices, our review found that, in a significant number of instances, the Laboratory failed to deactivate unneeded open computer ports such as USB and "firewire" ports that could have been used to circumvent security controls.

This weakness could have permitted the transfer of classified information to unclassified systems or easily concealable devices such as flash drives and portable hard drives. Open and unsecured ports also could have ultimately been used to transfer classified information to the Laboratory's unclassified network and the Internet. As evidenced by a series of e-mail exchanges in the March/April 2006 timeframe, officials in the Laboratory's Chief Information Officer's organization recognized that it would be a simple matter to exploit this weakness by plugging a USB or firewire recording device into an open port and copying information to it. However, despite this recognition, a Laboratory-wide solution was never developed or deployed.

Unlocked Computer Racks

We also noted that Laboratory system administrators failed to take advantage of readily available security measures that, in this case, could have helped prevent the unauthorized removal of the electronic classified material found on the seized flash drive. As part of an initiative to secure classified removable electronic media (CREM) following the 2002 security event, Los Alamos acquired locking mechanisms that were to be used to secure and prevent access to most rack-mounted classified computer systems. Following the installation of the locks, Laboratory management determined that if a computer system did not contain CREM and it was located in a vault-type room, there was no need to lock the racks. As a consequence, racks housing classified computers in the vault we reviewed were never secured. Based on our inquiries, a Laboratory management official conceded that using the available locks would have denied access to the enabled USB ports and could have prevented the download of the diverted classified information.

Inappropriate Access Granted

In addition, despite existing control measures and specific guidance by the NNSA to the contrary, system administrators at the Laboratory inappropriately granted certain individuals access to classified computer equipment to which they were not entitled. Specifically, individuals were given authority to physically access rack-mounted classified computer systems – access that could have permitted them to exploit open USB and firewire ports. Laboratory officials also allowed a person that had no need to print documents to use a high-speed classified network printer capable of producing double-sided documents identical to the

format of the hard copy classified documents that had been seized by law enforcement officials. A senior Laboratory security official confirmed that granting unneeded access to users was contrary to policy and that such action endangered security.

Introduction of Unapproved Devices

To ensure that classified systems are secure to operate, computers and peripheral devices should be evaluated for risk and included in an approved systems security plan prior to being introduced into a classified computing environment. However, program, security, and system administration officials responsible for the vault we reviewed routinely ignored these controls. Our review disclosed that officials permitted the introduction of several computers and peripheral devices (scanners and a printer) into a classified computing location even though these devices were not included in the accredited security plan. Thus, Laboratory and Federal officials were not able to evaluate the security implications of their inclusion in the vault in question. Potentially, the introduction of these devices could have compromised security.

Incompatible Security Functions

Additionally, Los Alamos did not adequately separate critical security duties. According to NNSA policy, "*measures must be implemented to ensure the management, control, and separation of security critical functions.*" However, Laboratory officials frequently did not provide for such separation, and a single individual was tasked with both system administration and security officer duties – essentially supervising and approving his or her own actions. As a result, the system administrator was able to provide access to classified computers and peripherals to unauthorized individuals, thereby overriding classified

protection safeguards. Los Alamos officials noted that the same issue existed in classified computing venues across the Laboratory.

ADDITIONAL FACTORS CONTRIBUTING TO DIVERSION

The security weaknesses we discovered resulted from control and management breakdowns at both the contractor and Federal level. While the Department, the NNSA, and Los Alamos had deployed some security controls to protect classified information, we observed problems with policy development and implementation. Had the Department and the NNSA been more aggressive in its contract administration and review activities, it may have been able to prevent, detect, or correct in a timely manner the problems or factors that contributed to the diversion of classified material.

Weaknesses in Security Policies

Our review, for example, disclosed a particularly significant instance where classified computer policies had not been developed or properly formalized. In 1999, the then Secretary of Energy directed that safeguards be developed and implemented to prevent the migration of classified data to unclassified systems to protect against insider threats. That 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.*" The requirement was never included in the Department's cyber security policy nor was it completely implemented by the Laboratory.

Furthermore, our inquiry revealed that conflicting direction and a lack of understanding regarding the introduction of equipment into classified computing environments contributed to the weaknesses we found. For example, Laboratory guidance required that security plans be updated and systems reaccredited when security configurations changed. Certain officials, however, incorrectly instructed security officers that there was no need to comply with that direction for selected devices. In other instances, officials inappropriately believed that the need to update security plans and obtain reaccreditation of classified systems was a matter solely within their discretion. They held this mistaken belief even though the Laboratory had published specific guidance regarding events that triggered update requirements. During our review, we identified a number of changes in security configurations for the vault we evaluated that should have triggered the requirement to update the system security plan. Yet, such action had not been taken.

Policy regarding the acquisition of computer support services for classified computing environments at the Laboratory was also inconsistent. In particular, as it applies to the matter under review, procurement policy permitted subcontractors to furnish unaccredited items such as scanners and software for archiving projects. Such practices, however, were contrary to the system's security plan and to cyber security guidance issued by the NNSA. The NNSA guidance specifically prohibited the connection of non-government owned equipment to classified networks.

Insufficient Management Review and Overdue Inspection Activities

The failure of Laboratory managers and Federal security officials to perform verification activities may also have adversely affected the classified security climate at the Laboratory and contributed to the recent removal of classified material. Laboratory security officials indicated that they did not visit vaults or computing facilities to determine whether controls described in security plans were actually in place. Federal officials at the Los Alamos Site Office also told us that they did not conduct physical inspections of the Laboratory's classified information systems. Accrediting officials at the Site Office explained that they placed a great deal of emphasis on reviewing security plans and accrediting systems, but that they had only 1.5 staff years to dedicate to classified security. They asserted that as a consequence they were unable to perform physical inspection of systems to validate that the Laboratory's plans were accurate and were being enforced.

Delays in completing classified information system inspections may also have impacted the detection of the security weaknesses we identified. NNSA officials informed us that they relied almost exclusively on the Office of Independent Oversight, Office of Health, Safety and Security to conduct detailed inspections of Los Alamos' classified information systems. These inspections are normally completed once every two years. However, the inspection at Los Alamos had not been performed for about four years for a variety of reasons including the 2004 security stand-down at the Laboratory. The Office of Independent Oversight had begun a previously scheduled review of Los Alamos' classified information systems at about the same time the diversion of classified information was discovered.

NEEDED ACTIONS

After this incident was discovered, management officials at various levels of the Department and at the Laboratory launched several efforts to identify and correct control deficiencies that caused or contributed to the unauthorized removal of classified information. In particular, the Secretary established two task forces to address our findings and the Deputy Secretary directed an immediate review of policies and practices related to computer ports at each of the Department's facilities.

As a result of our review, we provided the Department a number of recommendations designed to assist it in its efforts to correct identified deficiencies. For example, we recommended that the Department take immediate action to disable unneeded computer ports, secure classified computer racks, segregate critical security functions, and limit classified computer access and privileges to those who specifically require it.

In its letter of invitation, the Subcommittee requested that the Office of Inspector General identify broader actions that could improve the overall security climate at the Los Alamos National Laboratory and the Department at large. Based on the results of this special inquiry and other recent IG reviews and investigations, we concluded that the Department and the NNSA should:

1. Establish an up-to-date, unified, risk-based security policy that flows throughout all elements of the Department. It is essential that this policy be applied consistently and

that all aspects of security -- physical, cyber, and personnel -- be integrated to ensure a seamless system.

2. Aggressively hold individuals and institutions -- at the Federal and contractor levels -- accountable for failure to follow established security policies. Penalties should include meaningful reductions in contractor fees; personnel reassignments and terminations; civil penalties; program redirection; and, ultimately, should need be, contract termination.

One final note, one of the most disturbing aspects of this event is the fact that it was not discovered by the Laboratory but by local police during an off-site investigation unrelated to Laboratory activities. Without this inadvertent discovery, the diversion of classified material may never have been disclosed. In that light, Los Alamos and the Department need to strengthen efforts to proactively detect and prevent security breakdowns. This might include, for instance, improving the level of monitoring of classified computer/information activity by the use of specialized software, activity logging, and by initiating a program of unannounced security checks beyond routine inspections. Admittedly, there is a cost involved with such undertakings, but it is a cost that may be necessary given the pattern of security issues at the Laboratory.

Mr. Chairman, this concludes my statement and I would be pleased to answer any questions you may have.