Statement of Gregory H. Friedman

Inspector General

U.S. Department of Energy

Before the

Subcommittee on Oversight and Investigations

of the

Committee on Energy and Commerce

U.S. House of Representatives

FOR RELEASE ON DELIVERY
9:30 AM
Friday, April 20, 2007

Mr. Chairman and members of the Subcommittee, I am pleased to be here at your request to testify on the concerns expressed in your April 5th letter regarding operations at the Los Alamos National Laboratory.

Background

In January of this year, I testified before this Subcommittee on the special inquiry conducted by my office regarding the diversion of classified data from the Los Alamos National Laboratory. Specifically, at the request of the Secretary of Energy, we examined the efforts of the Department and its contractors to protect classified information and the steps that were taken to ensure that only authorized individuals had access to such information. Our report on this matter was issued on November 27, 2006.

Office of Inspector General Review

The Office of Inspector General (OIG) found that the security environment at Los Alamos was inadequate, despite the expenditure of millions of dollars by the National Nuclear Security Administration to upgrade various components of the Laboratory's security apparatus.

In particular, related to the cyber security control structure, 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 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, 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.

The OIG also reviewed certain aspects of the security clearance process in place for Laboratory employees. We identified particular weaknesses associated with this program which were discussed in a closed session of this Subcommittee in January of this year.

Departmental Response

After this incident was discovered, Department and Laboratory management officials launched several efforts to identify and correct control deficiencies that contributed to an environment in which classified information could be removed without authorization. In particular, the Deputy Secretary directed an immediate review of policies and practices related to computer ports at

each of the Department's facilities. Further, the Secretary established two high-level Task Forces to address our findings. The reports of the Secretary's Task Forces and a list of the proposed corrective actions were provided to my office last week.

The report from the Department's *Committee to Review the Cyber Security-related Recommendations* indicated concurrence with the OIG's report and specified that the Department had initiated corrective actions that involved revising policy, securing unneeded ports, limiting access and privileges, and maintaining separation of duties. The report also indicated that controls over security planning and accreditation and physical inspections were to be strengthened and that corrective actions would be tracked to resolution.

The *Personnel Security Program Review Task Force* analyzed the OIG report and agreed that there were personnel security program weaknesses. The Task Force addressed the security clearance issues raised in our November 2006 report. Specifically, it identified and developed recommendations for improving Department-wide training, policy, quality assurance and oversight, and organizational structure. Additional details are contained in the Task Force's report, which has been marked by the Department as "Official Use Only."

Many of the corrective actions outlined by the two Task Forces are in progress. However, implementation and execution are key. If properly carried out, the corrective actions should improve classified operations at Los Alamos and could help prevent similar incidents at Departmental facilities around the complex.

Issues Requiring Continuing Attention

As I have testified on several occasions, the Department must do a better job addressing the recurring challenges it faces. Specifically:

1. With regard to the current matter, the Department must ensure that all actions and recommendations outlined in the Task Force Reports are formalized into policy and adopted as practice throughout the Department. As part of that effort, these policies should be incorporated into all facility contracts.

2. To achieve the recommended reforms, the Department must establish firm schedules with specific implementation timelines and performance metrics.

3. Both Federal and contractor officials need to manage more aggressively. As part of that process, the Department needs to ensure that its Federal contract management function is adequately staffed and that the skill mix is appropriate. In addition, Department and Laboratory officials must develop a more comprehensive regimen of compliance testing and follow-up to ensure that security policies and procedures are rigorously followed.

4. Individuals and institutions, both Federal and contractor, must be held accountable for failure to follow established security measures. As it has begun to do in its response to the recent Los Alamos incident, the Department should emphasize that the failure to properly protect classified information and materials will have meaningful consequences.

Finally, consistent with our November 2006 recommendation, we continue to believe that the Department should perform a risk-based evaluation of cyber security funding at Los Alamos. The objective of this evaluation would be to ensure that the resources are available for complete implementation of the revised cyber security policies and procedures.

Ongoing Inspector General Efforts

For the past five years, we have identified both cyber and physical security as pressing management challenges. For these reasons, and because of the recent incidents, the Office of Inspector General continues to be concerned about security across the complex. We have ongoing activities to examine information technology and systems security; implementation of revised security measures; disposal of sensitive property; and, issues related to protective force training.

In addition to our on-going work, the full Committee, in January 2007, requested that the Government Accountability Office (GAO) examine the security of the Department's unclassified and classified information networks and its cyber security programs. My office coordinates closely with GAO on reviews of the Department, and we believe that the assessment requested by the Committee will lead to a strengthened agency-wide security posture. My office will continue to conduct audit, inspection, and investigative work that will complement the review requested by the Committee.

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