Department of Energy
Washington, DC 20585

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.

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