STATEMENT OF GREGORY H. FRIEDMAN
INSPECTOR GENERAL
U.S. DEPARTMENT OF ENERGY
SUMMARY
September 25, 2008

- Since 2002, the Office of Inspector General (OIG) has categorized information security as one of the Department of Energy's (Department) most significant management challenges. While incremental improvements have been made to improve security and reduce risks to systems and data, additional work needs to be done.

- The OIG recently issued a report on the certification and accreditation of the Department's national security information systems. Our review disclosed that weaknesses exist in the areas of risk management, security planning, and contingency planning. In addition, the National Nuclear Security Administration (NNSA) had not been fully successful in ensuring that its laboratories implemented the Department's updated, strengthened policies designed to protect national security information systems.

- A Fiscal Year 2008 review of the Department's unclassified cyber security program identified opportunities for improvements in areas such as certification and accreditation of systems, systems inventory, contingency planning and segregation of duties.

- The problems identified occurred because NNSA had not revised and implemented, in a timely manner, policies and guidance incorporating Federal and Departmental cyber security requirements. NNSA also had not effectively completed review and performance monitoring activities essential for evaluating the adequacy of cyber security operations.

- Since the end of Fiscal Year 2007, the Department has experienced a 45 percent increase in reported cyber security incidents. This significant increase demonstrates the need for sustained action in securing the Department's information systems.

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
10:00 AM
Thursday, September 25, 2008

Mr. Chairman and members of the Subcommittee, I am pleased to be here at your request to testify on matters relating to cyber security at the Department of Energy's (Department) national defense laboratories. These laboratories, which are part of the National Nuclear Security Administration (NNSA), possess and process some of the Department's most sensitive information; information which is critical to the Nation's defense.

Background

The Office of Inspector General (OIG) has a long-standing, proactive program to assess the effectiveness of the Department of Energy's cyber security strategy. Since 2002, the OIG has categorized information security as one of the Department's most significant management challenges. In April of 2007, I testified before this Subcommittee on the special inquiry conducted by my office regarding a diversion of classified data from the Los Alamos National Laboratory; an event made possible, in large part, by cyber security related weaknesses. The OIG has continued its efforts in this area by conducting a number of cyber security reviews throughout the Department, including NNSA and its national defense laboratories – Los Alamos, Lawrence Livermore, and Sandia.

Review of National Security Information Systems

In response to our special inquiry on the diversion of classified data at Los Alamos, the Department initiated a wide range of actions to address cyber security weaknesses related to

classified systems. For instance, the Department updated and strengthened its national security information systems policy for segregation of duties and system access techniques.

Earlier this year, we conducted an extensive review of the process to certify and accredit classified national security information systems at the NNSA laboratories. Certification and accreditation (C&A) is a critical part of the risk management process and is vital to understanding and mitigating cyber-related vulnerabilities. This process is designed to ensure that systems are secure prior to beginning operation and that they remain so throughout their lifecycle. It includes formal steps to: (1) recognize and address risks, (2) determine whether system security controls are in place and operating effectively, and (3) ensure that changes to systems are adequately tested and approved. Our findings relevant to the NNSA and its national defense laboratories revealed that:

- Critical security functions had not been adequately segregated, providing the opportunity for system security officers to gain access and modify systems without review or approval, creating an environment in which controls could be manually overridden;
- Risks associated with classified and unclassified systems operating in the same environment had not always been adequately evaluated. This weakness – exacerbated by the lack of segregation of duties – increased the risk that classified information could be transferred to unclassified systems;
- Users at one laboratory were allowed to manually change passwords, a practice specifically prohibited by the Department and one which rendered passwords on classified systems more susceptible to compromise;

- At the same laboratory, a number of security plans were not reviewed and approved by a Federal official, depriving NNSA of the opportunity to ensure that all risks to the systems were addressed;
- System security plans omitted information on hardware such as servers, network printers and scanners, the presence of which could have created a security vulnerability and enabled the unauthorized processing, diversion or theft of classified material. This condition paralleled one of our concerns related to the diversion of classified information at Los Alamos; and,
- Contingency plans outlining actions necessary to resume operations in the event of a disaster were not always developed or were incomplete.

The Department had strengthened policies designed to protect national security information systems in response to our recommendations following the Los Alamos incident. However, NNSA had not been fully successful in ensuring that its laboratories implemented these updated and stronger requirements. For example, two laboratories completed their C&A process using outdated requirements, leaving a number of systems vulnerable to control weaknesses such as the lack of segregation of duties and strong authentication techniques. In addition, Headquarters and field site officials had not effectively reviewed security plans to ensure that they were accurate and that they adequately addressed system risks.

Review of Unclassified Systems

The OIG has also devoted substantial resources to evaluating security measures designed to protect the Department's unclassified information systems and data. The Federal Information Security Management Act requires that agency Inspectors General conduct an annual independent evaluation of their Department's unclassified cyber security program and practices. Our recently issued Fiscal Year (FY) 2008 evaluation revealed a mixed-picture: on one hand, the Department had made incremental improvements in its unclassified cyber security program. For example, various sites had taken action to address weaknesses we identified during our FY 2007 evaluation by strengthening configuration management, updating policy, and incorporating cyber security performance requirements into management and operating contracts. However, a number of weaknesses that exposed systems to an increased risk of compromise still existed within the Department. This specifically included NNSA and its national defense laboratories. In particular:

- Two of the three defense laboratories had not yet completed certification and accreditation of certain business systems, a deficiency we first reported in FY 2006;
- System security plans at one laboratory did not include mandatory security controls. Such information is necessary for management to determine that all system risks have been fully considered and that mitigating controls are in place;
- At one laboratory, unneeded computer services had not been disabled on over 40 servers that hosted publicly accessible websites. These services, which in a number of instances could be accessed without the use of passwords or other authentication techniques, increased the risk of malicious damage to the servers and the networks on which they operated;

- All three laboratories had not yet completed the deployment of the Federally-mandated standard desktop configuration, an action that when implemented is intended to significantly enhance cyber-related controls;
- Computer incident reports did not always include information needed for reporting to law enforcement and for subsequent analysis for trending. Further, reported information was not always shared with other Department elements; and,
- At one laboratory, vulnerabilities were identified that may have allowed unsupervised foreign visitors to inappropriately access the site's intranet. Such practices, if exploited, could have permitted those individuals to probe the laboratory's network for vulnerabilities, implant malicious code, or remove data without authorization.

Issues Requiring Continuing Attention

While NNSA has taken steps to address a number of weaknesses identified in the past, additional action is necessary to protect systems and the information they contain from increasingly sophisticated and persistent attacks. Since the end of FY 2007, the Department has experienced a 45 percent increase in reported cyber security incidents. This significant increase demonstrates the need for sustained action in securing the Department's information systems.

Our work suggests that there are some recurring challenges that NNSA should consider as it moves forward. Specifically, NNSA should:

1. Implement, in a timely manner, all relevant Federal and Departmental cyber security requirements;

2. Strengthen the management review process by better monitoring field sites to ensure the adequacy of cyber security program performance; and,
3. Ensure that all outstanding cyber security weaknesses are corrected in a timely manner.

To achieve the recommended reforms as promptly as possible, NNSA should establish firm schedules with specific implementation timeframes and benchmarks.

Ongoing Inspector General Efforts

Both cyber and physical security continue to be pressing management challenges. For that reason, the Office of Inspector General has ongoing activities to examine information technology and systems security, implementation of physical security technology upgrades, protection of sensitive unclassified information, and accounting for nuclear materials in the hands of domestic licensees.

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