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
Friday, June 9, 2006

Mr. Chairman and members of the Subcommittee, I am pleased to be here at your request to testify on cyber security issues at the Department of Energy.

The Department of Energy, which spends over $2 billion each year on information technology (IT), has a current inventory of approximately 800 information systems, including up to 115,000 personal computers; many powerful supercomputers; numerous servers; and, a broad array of related peripheral equipment. These systems process operational, financial, and highly classified national security data. The need to protect this data and the related systems is of paramount concern to the Department and to the Office of Inspector General (OIG).

As is widely recognized both in the private and public sectors, the threat of intrusion or damage to information networks and systems continues to grow as cyber-related attacks become more sophisticated. The media regularly carries stories about malicious intrusions and compromises of sensitive data. Within the Department of Energy complex, on a regular basis, hackers attempt to intrude or cause damage to the Department's networks and systems. Cyber security threats of this sort reinforce the need for an aggressive Departmental program of controls and safeguards to protect against any compromise of vital data.

The Office of Inspector General has a proactive program to assess the effectiveness of the Department's cyber security strategy. For the last four years, the OIG has categorized information technology and systems security as one of the Department of Energy's most significant management challenges. This was based on internal control weaknesses

identified as part of the Inspector General's regular evaluation of the Department's cyber security program. These reviews include the annual evaluation required under the Federal Information Security Management Act (FISMA) and other cyber security-related reviews focusing on high-risk activities. In addition, the OIG's technology crimes unit, with its highly trained special agents, regularly and successfully investigates malicious attacks on Department systems.

In today's testimony I would like to highlight continuing challenges identified through our work in cyber security. I will outline results from completed activities and criminal investigations, and discuss ongoing review efforts.

2005 FISMA Evaluation

The purpose of the Federal Information Security Management Act of 2002 was to elevate attention to the issue of information technology security within the Federal sector. Under FISMA, each agency is required to develop, document, and implement an agency-wide program to provide security for the information and systems that support core operations. It also requires that agency Inspectors General conduct an annual independent evaluation of their Department's unclassified cyber security program and practices. At the Department, the evaluation is performed in conjunction with our annual Audit of the Department's Financial Statements and leverages testing of information technology controls performed on individual site and Department-wide financial systems.

Last year, as part of this evaluation, we conducted reviews at 27 sites, which, depending upon the location, included examinations of the Department's compliance with

information system-related laws and regulations; tests of general and application controls; and, vulnerability and penetration testing. We also incorporated information gathered by and conclusions reached by KPMG, our financial statement contractor; reports issued by the Government Accountability Office; inspection results obtained from the Department's Office of Independent Oversight; and, other internal studies.

Our 2005 review noted systemic cyber security problems that exposed the Department's critical systems to an increased risk of compromise. Specifically:

- The Department had not yet established a complete inventory of information systems; nor, had it identified all of the existing interfaces between internal and external systems and networks. These tasks are critical to planning and implementing protective efforts.

- Many sites had not completed or properly performed certification and accreditation of all their major and general support systems. This process verifies that the Department's systems are secure for operation and enables program officials to address high-risk issues through cost-effective mitigation strategies.

- The Department had not resolved noted problems with critical security controls such as access authority, segregation of duties, and configuration management. These safeguards and controls are designed to protect computer resources from unauthorized modification or loss and to prevent fraudulent activities.

- Contingency plans, necessary to ensure that systems could continue or resume operations in the event of an emergency, disaster, or malicious intrusion event, had not been completed for certain critical systems.

- Department elements did not always report cyber security incidents to law enforcement officials, as required. Failure to report these occurrences jeopardizes the timely investigation and resolution of these matters.

Similarly, our *Audit of the Department of Energy's 2005 Consolidated Financial Statements* (DOE/OAS-FS-06-01, November 2005) noted network vulnerabilities; weaknesses in access controls; and, other security shortcomings in the Department's unclassified computer information systems. These shortcomings increased the risk that malicious destruction, alteration of data, or other unauthorized processing could occur. As a result, "Unclassified Network and Information Systems Security" was designated as a reportable condition. An Information Technology Management Letter, which detailed 25 site-specific vulnerability findings, was issued as part of the 2005 Financial Statement Audit Report.

Criminal Investigations and Internal Control Weaknesses

As part of its law enforcement mission, the OIG aggressively pursues those who have attempted to compromise or inflict damage on the Department's computer systems. In this role, we have successfully investigated a number of intrusions with both national and international connections. We work closely with Department of Justice prosecutors and the Federal Bureau of Investigation in pursuing these matters and have worked on

specific cases with external law enforcement agencies such as New Scotland Yard and the Royal Canadian Mounted Police.

Because the Department has to deal with frequent intrusion attempts that could compromise systems, it is critical that strong security controls are implemented and appropriately executed. Our investigations have revealed problems with the deployment of controls in certain areas; for example, we have observed, in past investigations, a number of internal control weaknesses related to poor password administration. In one investigation, we determined that employees of a United States-based computer security company compromised unclassified Department of Energy and other government systems. Company officials were able to gain access to scientific data from a Headquarters system through the use of hacker tools that exploited a password vulnerability. Three individuals pled guilty in connection with those activities.

During another criminal investigation, we determined that two individuals within the United States gained access to an unclassified website belonging to Sandia National Laboratory, part of the Department of Energy's national laboratory network. They were able to gain access by exploiting a default password. These individuals pled guilty and have been sentenced in connection with their activities. In yet another investigation, an individual compromised a network at the Fermi National Laboratory, again by taking advantage of problems with weak password administration. The hacker, who pled guilty to his activities, used the system as his personal storage site to host illegal software – creating the ability for others to download the intruder's data from the Department's systems.

Ongoing Reviews

As noted previously, the Department invests over $2 billion each year for information technology throughout its complex. It is essential, especially given the size of the resource commitment, that all IT and cyber security initiatives be economic and efficient. To address this concern, we perform focused reviews on information technology-related areas. Over the course of such work, we have identified millions of dollars in potential savings in findings related to enterprise architecture, enterprise licensing, and IT support services.

The OIG is currently conducting comprehensive reviews directed at three key elements of cyber security: the Department's Systems Certification and Accreditation Process; its Cyber and Computer Forensics Analysis Capabilities; and, its Security Configuration and Vulnerability Management Program.

Systems Certification and Accreditation Process

Systems certification and accreditation is an essential step in verifying that the Department's systems are secure for operation. As noted previously, we identified multiple problems with the certification and accreditation process at certain sites; and, as a consequence, we initiated a review to determine whether the Department's systems have been appropriately certified and accredited for operation.

Cyber and Computer Forensics Analysis Capabilities

An ongoing effort is examining whether the Department had formally developed and implemented a unified, effective, and efficient means of analyzing and acting on information related to malicious attacks or intrusions. As part of this audit, we are following up on problems with cyber incident reporting previously identified by the OIG in 2003.

Security Configuration and Vulnerability Management

Building on findings in prior years and on the work already completed by our financial statement auditor, an audit team is examining operating systems and applications. This effort will determine, among other things, whether minimum security configuration standards have been established and implemented at Headquarters and Department field sites.

Status of the 2006 Office of Inspector General FISMA Evaluation

The Office of Inspector General is currently conducting the 2006 evaluation of the Department's Cyber Security Program. This Department-wide effort includes site-level evaluations – consisting of vulnerability and penetration testing and general and application controls testing – at eight sites: the NNSA Service Center in Albuquerque; Los Alamos National Laboratory; Sandia National Laboratories; the Chicago Operations Office; Argonne National Laboratory; the Kansas City Plant; the Y-12 Plant; and the National Energy Technology Laboratory. We are performing follow-up reviews at 12

additional sites. We are also specifically evaluating corrective actions and new initiatives begun this year by the Office of the Chief Information Officer.

As you are no doubt aware the Department of Veterans Affairs (VA) recently experienced the loss of sensitive personal data for millions of Veterans and, apparently, a large number of active duty personnel. This has understandably raised concerns about identity theft and related problems. My colleague, the Inspector General for the VA, has initiated several probes into this matter. As part of our ongoing FISMA evaluation, we intend to determine if the Department has taken action to prevent compromises similar to those which recently occurred at the VA.

Conclusion

The Department has informed us that, as a result of the concerns raised by our office, it has initiated actions to strengthen its cyber security program. In particular, under the direction of Secretary Bodman and Deputy Secretary Sell, it has implemented a number of countermeasures to reduce network vulnerabilities and embarked on a revitalization initiative that will focus high-level management attention on cyber issues. These efforts are promising and, if fully implemented, should help improve the Department's cyber security posture. While the Department is moving aggressively in this area, much remains to be done. As the House of Representatives Committee on Government Reform has recognized for the past three years through its ratings of Federal agencies' cyber security programs, significant weaknesses continue to exist at the Department of Energy.

The threat to the Department's systems is constantly evolving as hackers develop new and increasingly sophisticated tools and techniques. The potential for harm is not limited to malicious internet-based attacks, but also includes other efforts by internal users to gain access to resources or information to which they are not entitled. Constant vigilance is required to establish and maintain a defensive posture that is sufficient to prevent or quickly detect problems. The Office of Inspector General is committed to fulfilling its responsibilities by continuing to conduct a wide range of reviews to identify opportunities for improvement and investigate intrusion attempts on the Department's systems and networks.

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