SUMMARY

TESTIMONY OF
THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

JANUARY 30, 2007

- Over the last year, the Department has undertaken a major effort to improve our cyber security.

- In the last year we have updated the Department's cyber security policy, establishing a new governance structure for cyber security program management, and we have issued 15 guidance documents in specific cyber security areas. We are in the final review process for a revised National Security Systems Controls Manual, which updates the Department's formal directive for protecting classified systems.

- In direct response to the recent security incident at Los Alamos, the Deputy Secretary signed a memorandum in early November 2006 directing that actions be taken quickly to provide more protection of classified systems and the classified information on them. This memorandum included guidance prepared by the Office of the Chief Information Officer on blocking physical ports on classified computers.

- The Secretary has asked me to review the Inspector General's cyber security recommendations in his report on the recent Los Alamos incident. We have already been able to strengthen our cyber security directives based on a number of the lessons learned from this recent Los Alamos incident.

TESTIMONY OF
THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF ENERGY
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

JANUARY 30, 2007

Good morning, Mr. Chairman. My name is Tom Pyke. I am the Chief Information Officer of the Department of Energy. I came to the Department in November 2005, and have given a high priority to revitalizing the management of cyber security within DOE.

Over the last year, the Department has undertaken a major effort to improve our cyber security. We developed a plan to update Departmental cyber security directives and to issue guidance in specific areas of cyber security. In December 2006, the Deputy Secretary signed a new DOE cyber security Departmental Order which established a new governance structure for cyber security program management. This Order directs the use of a risk-based management approach and makes clear assignment of responsibility to Under Secretaries and other senior officials to oversee cyber security management within their organizations, including the field organizations under their jurisdiction. The Under Secretaries have accepted this enhanced role, and are working hard to strengthen the management of cyber security.

The new Order provides for timely issuance of urgently needed new cyber security guidance. To date I have issued 15 cyber security guidance documents, and the Office of the Chief Information Officer continues to develop guidance in accordance with the plan developed last year. I have already issued guidance on certification and accreditation of systems and on system configuration management, both directly relevant

to the recent Los Alamos incident. The new Order gives the Department flexibility to respond in a timely way to the changing threat environment and other time-sensitive concerns. For example, we have already issued special guidance on protection of personally identifiable information and on disposal of disk drives.

In direct response to the recent security incident at Los Alamos, the Deputy Secretary signed a memorandum in early November directing that actions be taken quickly to provide more protection of classified systems and the classified information on them. This memorandum included guidance prepared by the Office of the Chief Information Officer on blocking physical ports on classified computers. Our office has also conducted a study that has identified hardware and software means that can be used to block physical ports, or connection points, on computers. In addition, the Secretary has asked me to lead a review of the Inspector General's cyber security recommendations in his report on the recent Los Alamos incident. We expect to complete the report of this review by late February.

Finally, directly to the concerns being addressed in this hearing, we have recently completed a planned DOE National Security Systems Controls Manual, now in formal, final review within the Department. This Manual, which updates the Department's formal directive for protecting classified systems, was already being prepared when the Los Alamos incident became known. We have been able to incorporate actions in the Manual based on a number of the lessons learned from this incident.

I would be pleased to respond to any questions you may have.