

**Testimony of
David K. Garman
Under Secretary of Energy
U.S. Department of Energy
Before the
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
United States House of Representatives
June 9, 2006**

Mr. Chairman and Members of the Committee, I appreciate this opportunity to discuss the Department's efforts to strengthen our cyber security posture.

We recognize the importance of providing adequate protection to our systems and our data, given the criticality of those systems and data to supporting our mission as well as the sensitivity of much of the data in our possession. As such, we continue to assess and evaluate our cyber security posture as it relates to the threat.

Cyber security threats are on the rise. I cannot assert that we can fully protect all our data on our systems today; however, we try. Moreover, given the evolving and dynamic nature of the threat, it is unlikely that we will ever be fully satisfied with our cyber security posture. However, we must not allow the fact that we cannot achieve absolute, enduring protection against all cyber threats to deter us from undertaking serious, sustained efforts to improve our cyber security posture.

The Secretary and Deputy Secretary have made cyber security a priority. Shortly after they came to the Department, they grasped the challenge that confronted us. They recruited a new Chief Information Officer (CIO). They established a Cyber Security Executive Steering Committee on which I serve, along with the Administrator for the National Nuclear Security Administration, the CIO, and others. We have established a Cyber Security Working Group comprised of information technology and cyber security specialists to assist us in our responsibilities. During the ensuing months, we have developed and issued a Cyber Security Revitalization Plan that we are currently implementing.

To put it bluntly, while we are not yet where we need to be, I believe we are far better off than we were a year ago.

In addition to stressing the importance of cyber security to the Assistant Secretaries and Program Directors who report to me, I have met with the cyber security and information technology personnel who report to them to discuss the particular challenges that they face. We have also recently detailed a cyber-security expert to my office to assist me in implementing the plan and identifying best practices for replication.

Therefore, in addition to the efforts embodied in the Cyber Security Revitalization Plan, we have engaged in a number of activities that improve the Department's ability to protect its data.

For example, in 2005, our Office of Science initiated a cyber security Site Assistance Visit (SAV) Program. Cyber security specialists from the Office of Science, together with inspectors from the Office of Security and Safety Performance Assurance, are conducting cyber security reviews at various sites and national laboratories. These visits are helping sites to identify and remediate potential weaknesses, accept risks, and establish a consistent cyber security baseline. In addition, these visits serve to provide training to a cadre of cyber security personnel and help identify best practices. To date, the Office of Science has conducted ten such visits and will shortly expand coverage to facilities outside the purview of the Office of Science.

The Office of Environmental Management (EM) has also made significant progress in re-engineering its cyber security management oversight process. EM has developed several cyber security management applications such as an Intrusion Detection Monitoring capability, allowing them to identify foreign-based cyber attacks launched against EM facilities from the Internet, and a Risk Assessment Management System, which automates cyber security risk assessments in support of their certification and accreditation responsibilities.

Those are just some examples. All of our programs have active cyber security programs in place, and all are working collaboratively to implement relevant portions of the Cyber Security Revitalization Plan at Headquarters and in the Field. We know this is not a quest for an end point where we declare success, but rather, a continuous process where we strive to get ahead, and stay ahead of our adversaries.

Just as we welcome the efforts of the Inspector General, the Office of Security and Safety Performance Assurance, and others to test and evaluate our success in this regard, we welcome the efforts of this subcommittee as we work to manage cyber security risk in a cost- effective and responsible manner.

This concludes my testimony. I would be pleased to respond to any questions you might have, either today or in the future.