STATEMENT OF

KEVIN M. KOLEVAR

ASSISTANT SECRETARY FOR ELECTRICITY DELIVERY AND ENERGY RELIABILITY

U.S. DEPARTMENT OF ENERGY

BEFORE THE

SUBCOMMITTEE ON ENERGY AND AIR QUALITY

COMMITTEE ON ENERGY AND COMMERCE

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 11, 2008

Mr. Chairman, members of this committee, thank you for the opportunity to testify before you today on this critically important matter.

This hearing addresses more that just a reliability concern but a national security concern. The Department of Energy and FERC and the electric sector must work cooperatively towards eliminating cyber vulnerabilities in control systems and preventing malicious cyber attacks on our electric infrastructure. Our nation's electric power grid must be better protected – we must harden our power system.

The Department of Energy regularly discovers new vulnerabilities in the control systems employed by many utilities. This is not hyperbole, let me assure you that cyber

attacks against control systems have occurred and they are becoming increasingly sophisticated.

The Director of National Intelligence, J. Michael McConnell, only underscored these concerns when he acknowledged earlier this year that cyber exploitation has not only grown more sophisticated, but more targeted, and more serious. Embedded processors and controllers in critical sectors are being targeted for exploitation and potentially for disruption or destruction with increasing frequency by a growing number of adversaries, not all of whom are in the pay of foreign governments.

According to one senior CIA analyst, some cyber intrusions into utilities have been followed by extortion demands. Cyber attacks have been used to disrupt power equipment in regions outside the United States. And, in at least one case, a cyber-based disruption caused an outage that affected multiple cities.

And because these cyber attacks are conducted over the Internet, they can be launched from just about anywhere, by anyone with a phone line and a modem.

However, while small groups or even individuals could execute limited attacks, a nationwide attack probably would require significant national level resources. Nevertheless, the consequences of a cyber attack on the electric sector are potentially significant, across a host of issues. For that reason, a limited role for the federal government is warranted if the nation's energy infrastructure is to be protected. The nation cannot function without reliable supplies of electricity. Our homes, our communities, our businesses – even the government itself – depend heavily, almost exclusive, on a functioning grid. And we must be increasingly vigilant in our efforts to protect that grid from cyber attacks. To be clear, we must focus on 1) identifying and

eliminating vulnerabilities, 2) improving intelligence gathering and communication of threat information and 3) we must evaluate overall risk and swiftly respond to potential emergencies.

The Department has been substantively engaged on this issue for some time. In 2003, DOE's Office of Energy Assurance, the predecessor program to the current office of Electricity Delivery and Energy Reliability, was designated to work directly with energy owners and operators to protect energy infrastructures from all hazards and help make them become more resilient.

DOE does this by applying sound risk management practices that assess potential weaknesses and we implement physical and cyber solutions to mitigate the risks based on the vulnerabilities we identified.

Under the National Infrastructure Protection Plan's partnership framework, the Department works intimately with the private sector through the Electricity Sector Coordinating Council and the Oil and Natural Gas SCC. In this role, the Department maintains a network of cyber security stakeholders in the private sector and federal, state, local, tribal, and territorial governments.

And this work has spoken directly to cyber concerns. In 2005, the Department collaborated with DHS and Natural Resources Canada to work directly with energy sector asset owners and operators to develop the *Roadmap to Secure Control Systems in the Energy Sector*, a detailed, prioritized plan for cyber security improvements in control systems over the next 10 years.

This effort built trust with the energy sector and has since spawned numerous collaborative efforts to enhance control systems security. More than 100 public and

private projects in the energy sector have been aligned with the Roadmap goals. Control systems cyber security projects funded by the Department of Energy alone have more than 35 private sector partners teaming up with national laboratory researchers.

To date, the Department and its national laboratories have conducted test bed and on-site field assessments of 15 common control systems used widely across the energy sector. These assessments have revealed vulnerabilities ranging in severity from minimal to high impact. Some were one of a kind and were corrected quickly and with relative ease. Others are common to systems found around the country and around the globe, making efforts to address them more complex. In either case, the Department has worked and will continue to work with vendors and asset owners to correct deficiencies, develop security patches and, if needed redesign systems in order to eliminate the identified vulnerability.

The vendors with whom we work are also working to contain the threats. They have developed six next-generation "hardened" systems —one vendor has seen 21 of their hardened systems deployed in the marketplace. And they have released countless software patches to secure legacy systems better.

The Department uses its vulnerability analysis and mitigation to aid the energy sector in implementing sound risk management. Through our national laboratories the Department has conducted cyber security training for more than 1,700 asset owners, operators, and security vendors.

Using knowledge from test bed assessments, the Department educates these end users on cyber security best practices and implementing system fixes and vulnerability mitigation strategies. The Department publishes a periodic "Common Vulnerabilities"

report to educate asset owners and operators on the most common vulnerabilities discovered and actions they can take to mitigate those vulnerabilities on their own systems.

By working directly with vendors and end users for system testing and security training, we have seen an increase in the quality of the partnerships and connections we have developed with the energy sector over the past five years. We understand that securing the energy sector requires maintaining open and close communication with private sector asset owners and operators, who own more than 85 percent of the nation's energy sector assets.

We are vigilant – but our comprehensive understanding of the nature of the threat we face must be updated on a continuing basis. The Department of Energy has long been a source of credible threat information for the nation's energy community. It is part of our job to help them prioritize risk and respond appropriately.

We are constantly leveraging an extensive intelligence-gathering network, proven methodologies, and highly skilled professionals to assess and interpret threat information. With 17 testing facilities from five Department of Energy National Laboratories, we have at our hands field-scale operational and multi-sector control systems for risk assessment, vulnerability testing and advanced modeling and simulation of the impacts and consequences of a cyber attack.

In addition, I am confident we have the necessary intelligence information, analysis capabilities, technical expertise and energy industry relationships to enable us to respond to emerging threats quickly and to make informed decisions that will keep the grid protected, whether problems are the result of cyber attacks or not.

The Administration is continuing to examine what additional authorities are appropriate for DOE and FERC. To the extent that Congress acts in this area, we recommend that it consider the following:

Allow the FERC to establish Interim Reliability Standards for the purpose of rapidly responding to specific electric sector vulnerabilities.

When presented with a credible cyber security threat against the bulk power system, such interim reliability standards could provide an effective bridge until being replaced by cyber security reliability standards developed, approved and implemented pursuant to section 215.

With respect to potential measures in the face of an imminent threat the bulk power system, allow the Department of Energy to issue an order for immediate remedial action. That order could stand until new FERC interim standards, or standards developed pursuant to section 215 were put into place.

The authority to issue emergency cyber security actions is very similar to the Secretary of Energy's existing authority to issue emergency interconnection orders under section 202 of the Federal Power Act. Since 1977, when the Department of Energy Organization Act created both DOE and FERC, the FPA section 202 authority has been vested in DOE. Throughout Administrations involving several different Presidents and of both parties, the Department has used this authority judiciously but effectively to address particular situations in which such an order was necessary to help ensure reliable supplies of electric energy. The Department has demonstrated that, as circumstances warrant, it can exercise the section 202 emergency interconnection authority very quickly.

At this time, Mr. Chairman, I would like to submit my prepared statement for the record and I would be happy to take any questions you may have.