STATEMENT OF

PATRICIA HOFFMAN

ASSISTANT SECRETARY

OFFICE OF

ELECTRICITY DELIVERY AND ENERGY RELIABILITY

U.S. DEPARTMENT OF ENERGY

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES

UNITED STATES SENATE

May 5, 2011

Chairman Bingaman, Ranking Member Murkowski and members of the Committee, thank you for this opportunity to discuss the cyber security issues that face the electric industry, as well as proposed legislation intended to strengthen protection of the bulk power system and electric infrastructure from cyber security threats.

Title XIII of the Energy Independence and Security Act of 2007 (EISA) states, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure." The protection and resilience of critical national infrastructures is a shared responsibility of the private sector, government, communities, and individuals. As the complexity, scale, and interconnectedness of today's infrastructures have increased, it has changed the way services and products are delivered, as well as the traditional roles of owners, operators, regulators, vendors, and customers.

Ensuring a resilient electric grid is particularly important since it is arguably the most complex and critical infrastructure that other sectors depend upon to deliver essential services. Over the past two decades, the roles of electricity sector stakeholders have shifted: generation, transmission, and delivery functions have been separated into distinct markets; customers have become generators using distributed generation technologies; and vendors have assumed new responsibilities to provide advanced technologies and improve security. These changes have created new responsibilities for all stakeholders in ensuring the continued security and resilience of the electric power grid.

Cyber security Activities and Accomplishments

For more than a decade, the Department of Energy's Office of Electricity Delivery and Energy Reliability (OE) has been substantively engaged with the private sector to secure the electric grid. In December 2003, the Homeland Security Presidential Directive 7 (HSPD-7) designated the Department as the sector-specific agency (SSA) for the energy sector responsible for collaborating with all federal agencies, state and local governments, and the private sector. As the SSA, OE, representing the Department, works closely with the private sector and state/Federal regulators to provide secure sharing of threat information, to collaborate with industry to identify and fund gaps in infrastructure research, development and testing efforts, to conduct vulnerability assessments of the sector, and to encourage risk management strategies for critical energy infrastructure.

The 2010 *National Security Strategy* underscores the need to strengthen public-private partnerships in order to design more secure technology that will better protect and improve the resilience of critical government and industry systems and networks. OE has long recognized that neither government, nor the private sector, nor individual citizens can meet cyber security challenges alone. In 2006, OE facilitated the development of the *Roadmap to Secure Control Systems in the Energy Sector* to provide a detailed collaborative plan for improving cyber security in the energy sector and concrete steps to secure control systems used in the electricity and oil and natural gas sectors. The plan calls for a 10-year implementation timeline with a 5-year update scheduled for release in the summer of 2011. To implement the priorities in the

Roadmap, the Energy Sector Control Systems Working Group (Working Group) was formed and comprised of cyber security and control systems experts from government, the electricity sector, and the oil and natural gas sector.

Since 2006, the *Roadmap* has provided a collaborative strategy for prioritizing cyber security needs and focusing actions under way throughout government and the private sector to ensure future energy system security. The *Roadmap* goals and strategy have also been fully integrated into the *Energy Sector-Specific Plan*. Since the *Roadmap* was released, important progress has been made in improving cyber security in the energy sector. These improvements have benefited existing systems and are contributing to the secure design and integration of advanced systems that incorporate smart grid technologies.

Through competitive solicitations and partnerships with industry, academia and national laboratories, OE has supported the development of several advanced cyber security technologies that are now commercially available within the energy sector:

- A technology to secure serial communications for control systems, based on the Secure Supervisory Control and Data Acquisition (SCADA) Communications Protocol developed by the Pacific Northwest National Laboratory – the technology is rapidly being adopted by utilities.

- Software toolkits that let electric utilities audit the security settings of SCADA systems – the software is available for download from the vendor website. The latest release addresses the Inter-Control Center Communications Protocol (ICCP) which is used for utility-to-utility communications – a high-risk attack vector.

- Monitoring modules that aggregate security events from a variety of data sources on the control system network and then correlate the security events to help utilities better detect cyber attacks.

- An Ethernet security gateway, based on an interoperable design developed by Sandia National Laboratories, that secures site-to-site Ethernet communications and protects private networks.

OE established the National SCADA Test Bed in 2003 to provide a national capability for cyber security experts to systematically evaluate the components of a functioning system for inherent vulnerabilities, develop mitigations, and test the effectiveness of various cyber security technologies. Major accomplishments include:

- Completed vulnerability assessments of 38 SCADA systems and provided mitigation recommendations. As a result, vendors have implemented many of the recommendations in “hardened” next-generation SCADA systems that are now commercially available and being deployed in the power grid.

- Utility groups have also formed partnerships to fund additional cyber security assessments at the test bed to address specific cyber security concerns.

- Provided advanced cyber security training for over 2300 representatives from over 200 utilities to demonstrate how to detect and respond to complex cyber attacks on SCADA systems.

- Developed the "Common Cyber Security Vulnerabilities Observed in Control System Assessments" report to help utilities and vendors mitigate vulnerabilities found in many SCADA systems. OE has also worked with the North American Electric Reliability Corporation (NERC) to develop the *Top Ten Vulnerabilities of Control Systems and their Associated Mitigations* report in 2006 and 2007.

OE is also working closely with academic and industry partners through the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG), which is a University led public-private research partnership supported by the OE, Department of Homeland Security (DHS), and Industry for frontier research that supports resilient and secure smart grid systems. TCIPG leverages and expands upon previous research funded primarily by the National Science Foundation. TCIPG research focuses on building trusted energy delivery control systems from un-trusted components, and transitioning next-generation cyber security technologies to the energy sector. As an example, TCIPG released the Network Access Policy Tool that is now being used by industry and asset owners to characterize the global effects of local firewall rules in control system architectures. The tool will help utilities better manage and maintain security on their highly-complex communications networks.

Just recently, OE launched several new initiatives to enhance cyber security in the energy sector.

- OE established the National Energy Sector Cyber Security Organization (NESCO)—a cost-shared private sector organization—to enhance information sharing through public-private partnership on cyber vulnerabilities, threats, and best practices across the sector, to analyze threats to the sector, and to identify gaps in existing standards.

- OE, in coordination with DHS and other Federal agencies, has conducted several cyber threat information sharing workshops to analyze classified information, determine the impact to the sector, and develop mitigations that were specifically designed to work in the sector. This cooperative process has proven to be more effective and accepted than dictating solutions to the sector.

- OE, in coordination with the National Institute of Standards and Technology (NIST) and NERC, is leading a collaborative effort with representatives from across the public and private sectors to develop a cyber security risk management guideline. The objective of this effort is to provide a consistent, repeatable, and adaptable process for the electric sector, and enable organizations to proactively manage risk.

Ensuring the cyber security of a modern, digital electricity infrastructure is a key objective of national smart grid efforts. As a result, a number of key initiatives have been developed to ensure future system security and enable the energy sector to better design, build, and integrate smart grid technologies. OE has engaged in partnerships to perform these activities with key organizations including Federal Energy Regulatory Commission (FERC), the U.S. Department

of Commerce, NIST, DHS, the Federal Communications Commission, the Department of Defense (DoD), the intelligence community, the White House Office of Science and Technology Policy, state public utility commissions, the National Association of Regulatory Utility Commissioners, NERC, the Open Smart Grid Subcommittee, Electric Power Research Institute (EPRI), and other energy sector organizations.

The American Recovery and Reinvestment Act of 2009 accelerated the development of smart grid technologies in grid modernization efforts by investing in pilot projects, worker training, and large scale deployments. This public-private investment worth over $9.6 billion was dedicated to a nationwide plan to modernize the electric power grid, enhance the security of U.S. energy infrastructure, and promote reliable electricity delivery. The $4.5 billion in Recovery Act funds, managed by OE, was leveraged by $5.1 billion in funds from the private sector to support 132 Smart Grid Investment Grant and Smart Grid Demonstration Grant projects across the country. Each project awardee committed to implementing a cyber security plan that includes an evaluation of cyber risks and planned mitigations, cyber security criteria for device and vendor selection, and relevant standards or best practices the project will follow.

As called for in Section 1305 of EISA, OE is collaborating with NIST and other agencies and organizations to develop a framework and roadmap for interoperability standards which includes cyber security as a critical element. As part of this effort, NIST established the public-private Smart Grid Interoperability Panel, and within that the 450-member Cyber Security Working Group (CSWG) to lead the development of cyber security requirements for the smart grid. After engaging members in numerous workshops and teleconferences and following two formal reviews, the CSWG released the first version of its *Guidelines for Smart Grid Cyber Security*. The three-volume document details a strategy that included smart grid use cases, a high-level smart grid risk assessment process, smart grid specific security requirements, development of a security architecture, assessment of smart grid standards, and development of a conformity assessment program for requirements.

To address cyber security needs for smart grid technologies, OE partnered with leading utilities and EPRI to develop cyber security profiles for major smart grid applications – Advanced Metering Infrastructure, Third-Party Data Access, and Distribution Automation. These profiles provide vendor-neutral, actionable guidance to utilities, vendors and government entities on how to build cyber security into smart grid components in the development stage, and how to implement those safeguards when the components are integrated into the power grid. These documents support the NIST "Cyber Security Guidelines for the Smart Grid" NISTIR – 7628. OE also co-chairs the NIST CSWG.

Senate Energy and Natural Resources Committee Proposed Legislation

The proposed bill includes provisions intended to strengthen the bulk power system and electric infrastructure by addressing cyber security vulnerabilities and protecting against cyber security threats by adding a new section to the Federal Power Act (FPA). While the Administration does not yet have a position on the bill, the Department offers the following observations.

To begin with, the proposed bill correctly indentifies, defines, and distinguishes between a cyber security vulnerability and a cyber security threat. These are two related, but different concepts.

Vulnerabilities need to be indentified and addressed, while threats need to be protected against. Given that distinction, it is appropriate that FERC and NERC, with their reliability standards responsibilities, be the entities that are responsible for addressing cyber security vulnerabilities. In that regard, references in the proposed bill to "protecting critical electric infrastructure from cyber security vulnerabilities" should be changed to "addressing critical electric infrastructure cyber security vulnerabilities."

In addition, Section 224(a)(1) defines critical electric infrastructure to include distribution assets that affect interstate commerce. This significantly expands FERC's jurisdiction for setting reliability standards beyond the bulk power system as provided in FPA section 215.

Also, Section 224(f) would require a comprehensive plan identifying emergency measures to protect the reliability of the electric power supply of national defense facilities located in Alaska, Hawaii, and Guam in the event of an imminent cyber security threat. Pertinent to that, in July 2010, DOE and DoD signed a memorandum of understanding (MOU) "Concerning Cooperation in a Strategic Partnership to Enhance Energy Security". The purpose of the MOU is to enhance national energy security and demonstrate Federal Government leadership in transitioning America to a low carbon economy. This MOU provides an opportunity to develop a comprehensive approach that reduces the impact of power loss to defense critical assets, considering both mitigation and response measures to ensure vital defense capabilities are not disrupted.

Finally, the legislation does not yet address a unique, sensitive cyber security information disclosure problem faced by Federal Power Marketing Administrations subject to both the Freedom of Information Act (FOIA) and mandatory reliability standards enacted under Section 215 of the Federal Power Act. This sensitive information, once disclosed as required by the mandatory reliability standards, appears not to be protected from public disclosure under the FOIA. This security vulnerability could be avoided if legislative language were included to amend FOIA Exemption 3 so that, "A Federal agency subject to mandatory reliability standards enacted pursuant to Section 215 of the Federal Power Act shall not disclose critical asset information unless the disclosure is: (1) pursuant to requirements approved by the Federal Energy Regulatory Commission under Section 215 of the Federal Power Act, or (2) in compliance with open access tariffs approved by the Federal Energy Regulatory Commission, or (3) determined by the agency to be necessary to maintain system reliability." Definitions of "critical asset," "bulk power system," and "critical asset information" have been drafted and also should be included to limit the focus to electric reliability.

Conclusion

In conclusion, I would like to again thank this Committee for its leadership in supporting the protection of the bulk power system and critical electric infrastructure against cyber security threats. Recognizing the interdependencies between different sectors, it is important to have a comprehensive strategy for cyber security legislation. DOE would be happy to work with the Committee on this legislation.

I would be pleased to address any questions the Committee might have.