STATEMENT OF

PATRICIA HOFFMAN

ASSISTANT SECRETARY

OFFICE OF

ELECTRICITY DELIVERY AND ENERGY RELIABILITY

U.S. DEPARTMENT OF ENERGY

BEFORE THE

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON ENERGY AND POWER

UNITED STATES HOUSE OF REPRESENTATIVES

May 31, 2011

Chairman Whitfield, Ranking Member Rush and members of the Subcommittee, thank you for this opportunity to discuss the cyber security issues facing the electric industry, as well as potential 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.

The Department of Energy's Office of Electricity Delivery and Energy Reliability (OE) supports the Administration's strategic comprehensive approach to cyber security, focusing on the following key areas: public-private partnerships to accelerate smart grid cyber security efforts; research and development of advanced technology to create a secure and resilient electricity infrastructure; cyber security standards to provide a baseline to protect against known vulnerabilities; facilitating timely sharing of relevant and actionable threat information; risk management frameworks with private sector risk management plans subject to performance evaluation; incident management and response; and development of a highly skilled and adaptive workforce.

Cyber security Activities and Accomplishments

For more than a decade, the 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 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. This technology is rapidly being adopted by utilities.

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

- 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 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, 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, working with the National Institute of Standards and Technology (NIST), DHS, the Federal Energy Regulatory Commission (FERC), 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 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 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 that 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 includes 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.

DOE Comments on Proposed Legislation

The Administration has proposed comprehensive cyber security legislation which was transmitted to May 12, 2011, (http://www.whitehouse.gov/omb/legislative_letters) focused on improving cyber security for the American people, our Nation's critical infrastructure, and the Federal Government's own networks and computers. Specifically, the Administration proposes the following changes to current law to enhance protection of critical infrastructure:

1) Voluntary government assistance to industry, states, and local government to improve the Government's (DHS and sector specific agencies) ability to provide technical support, share cyber security information and expertise available to state and local governments and the private sector on request and on a voluntary basis with appropriate legal, privacy, and civil liberties safeguards.
2) Voluntary information sharing with industry, states, and local government to remove barriers that hinder voluntary sharing of cyber security information between the government and industry for cyber security purposes, and help improve overall situational awareness of threats and vulnerabilities in cyberspace.
3) Critical infrastructure cyber security risk mitigation to create a flexible framework for enhanced cooperation between the Government and critical infrastructure operators nationwide.

The Administration looks forward to working with Congress to enact these legislative changes..

We also understand that the Committee is currently considering reintroduction of "The Grid Reliability and Infrastructure Defense Act" (GRID Act). The Administration has no formal position on this legislation, and as noted above, we have a proposal of our own that we believe provides the best and most effective course of action. At the Committee's request, we are providing the following observations on existing authorities.

Processes for the development of risk frameworks, risk management plans, and implementation of performance evaluations for electric grid cyber security should be consistent with the Administration's cyber security legislation proposal. The Administration's proposal seeks to improve cyber security across the range of critical infrastructure sectors, while also recognizing the unique requirements for resilience and reliability and the important roles, responsibilities, and resources of the government and private sector entities within the electric sector.

Conclusion

In conclusion, I would like to again thank this Subcommittee 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, government-wide strategy for cyber security legislation. DOE looks forward to working with Congress to enact comprehensive cyber security legislation that will enhance the protection of critical infrastructure as specified in the Administration's bill.

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