STATEMENT OF
PATRICIA HOFFMAN
ACTING ASSISTANT SECRETARY
FOR ELECTRICITY DELIVERY AND ENERGY RELIABILITY
U.S. DEPARTMENT OF ENERGY
BEFORE THE
COMMITTEE ON ENERGY AND NATURAL RESOURCES
U.S. SENATE

MAY 7, 2009

Mr. Chairman and members of the Committee, thank you for this opportunity to testify before you on the cyber security issues facing the electric industry and on emergency authorities to protect critical electric infrastructure. All of us here today share a common concern that vulnerabilities exist within the electric system and that the government and the private sector must do everything we can to address it. This is particularly true for smart grid systems, which by their very nature involve the use of information technologies in areas and applications on the electric system where they have not been used before. With the funding provided for smart grid activities in the American Recovery and Reinvestment Act of 2009, the Department will be expanding our partnership with industry to advance the smart grid while maintaining security of smart grid devices and systems.

A smart grid uses information technology to improve the reliability, availability, and efficiency of the electric system. With smart grid, information technologies are being applied to electric grid applications including devices at the consumer level through the transmission level to make our electric system more responsive and more flexible.

To be clear, the smart grid is both a means to enhancing grid security as well as a potential vulnerability.

Enhanced grid functionality enables multiple devices to interact with one another via a communications network. These interactions make it easier and more cost effective, in principal, for a variety of clean energy alternatives to be integrated with electric system planning and operations, as well as for improvements in the speed and efficacy of grid operations to boost electric reliability and the overall security and resiliency of the grid. The communications network, and the potential for it to enhance grid operational efficiency and bring new clean energy into the system, is one of the distinguishing features of the smart grid compared to the existing system.

For example, Wide Area Measurement Systems (WAMS) technology is based on obtaining high-resolution power system measurements (e.g., voltage) from sensors that are dispersed over wide areas of the grid. The data is synchronized with timing signals from Global Positioning System (GPS) satellites. The real-time information available from WAMS allows operators to detect and mitigate a disturbance before it can spread and enables greater utilization of the grid by operating it closer to its limits while maintaining reliability. When Hurricane Gustav came ashore in

Louisiana in September 2008, an electrical island was formed in an area of Entergy's service territory. Entergy used the phasor measurement system to detect this island, and the phasor measurement units (PMU) in the island to balance generation and load for some 33 hours before surrounding power was restored.

The Department understands that the smart grid will be more complex than today's grid, with exponentially more access points, both virtual and physical through smart grid devices and without proper controls in place these factors could result in increasing the electric sector's vulnerabilities.

Department of Energy Activities:

The mission of the Office of Electricity Delivery and Energy Reliability is to lead national efforts to modernize the electric grid, to enhance the security and reliability of the energy infrastructure, and to facilitate recovery from disruptions to the energy supply. To accomplish this mission, the Office focuses on long-term system requirements through our research investments in the electricity delivery system and near-term energy vulnerability assessments/disaster recovery. Our efforts to enhance the cyber security of the energy infrastructure have produced results in five areas. We have

- Identified cyber vulnerabilities in energy control systems and worked with vendors to develop hardened systems that mitigate the risks
- Developed more secure communications methods between energy control systems and field devices
- Developed tools and methods to help utilities assess their security posture
- Developed a modeling and simulation capability to estimate the effects of cyber attacks on the power grid
- Provided extensive cyber security training for energy owners and operators to help them prevent, detect, and mitigate cyber penetration.

In 2005, the Department (in collaboration with the Department of Homeland Security and Natural Resources-Canada) worked directly with asset owners and operators in the oil, gas, and electricity sectors to develop the *Roadmap to Secure Control Systems in the Energy Sector* – a detailed, prioritized plan for cyber security improvements over the next 10 years, including best practices, new technology, and risk assessment. The Roadmap vision states that in 10 years, controls systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function. Industry representatives defined goals, milestones, and priorities to guide the industry toward this vision.

As a result, the Department was one of the first research organizations to align its cyber security research activities with the Roadmap goals and vision. The Institute for Information Infrastructure Protection (I3P) is working to develop several technologies that address Roadmap goals including security metrics and trusted devices. The Trusted Cyber Infrastructure for the Power Grid (TCIP) (a collaboration of universities led by the University of Illinois at Champaign-Urbana working with energy sector asset-owners and operators and vendors with funding from NSF, DOE, and DHS) is also conducting extensive cyber security research that

aligns with the Roadmap goals. In addition, there are over 50 other public and private organizations working on projects that directly address the challenges identified in the Roadmap.

Efforts at the national labs are also producing results that industry can use today to enhance the security of their control systems. For example, Sandia National Laboratories developed the Advanced Network Toolkit for Assessments and Remote Mapping, or ANTFARM. This tool aids energy utility owners in mapping critical cyber assets and access points to allow easy visualization of their control system networks-a critical step in meeting the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards. Released in August 2008. The toolkit is open source and available online for free.

Through the Department's National Supervisory Control and Data Acquisition (SCADA) Test Bed program, we have assessed 90% of the current market offering of SCADA and energy management systems (EMS) in the electric sector, and 80% of the current market offering in the oil and gas sector. Twenty test bed and on-site field assessments of control systems from vendors including ABB, Areva, GE, OSI, Siemens, Telvent, and others, have led them to develop 11 hardened control system designs with thirty-one of these systems now deployed in the marketplace. Vendors also have released several software patches to better secure legacy systems. The National SCADA Test Bed (NSTB) is a state-of-the-art national resource designed to aid government and industry in securing their control systems through vulnerability assessments, focused research and development (R&D) efforts, and outreach. Over the years the Department has expanded its investments in the NSTB and today it includes the resources and capabilities of five national laboratories (Idaho National Engineering Laboratory, Sandia National Laboratory, Pacific Northwest National Laboratory, Oak Ridge National Laboratory, and Argonne National Laboratory) as well as many cost-shared projects with the private sector.

The national labs also educate end-users on cyber security best practices and implementing methods to better manage control systems risk. For example, the Idaho National Laboratory has released on an annual basis a "Common Vulnerabilities" report. Using results from assessments performed from 2003 to 2007, the November 2008 document represents a steadily growing understanding of control system security issues and methods for mitigating current and emerging vulnerabilities. This effort is expanding to new technologies, such as substation automation and Smart Grid, as the program seeks a continuing understanding of the systems being planned for and deployed in the energy sector critical infrastructure.

The Department, through a work-for-others agreement with the Idaho National Laboratory, is also working with a major vendor of smart meters to conduct a cyber security assessment of their device. The primary motivation for this work was driven by the utilities - end-users of the product.

The Department has also funded several research and development projects with the private sector. The Bandolier project, led by Digital Bond, is developing security audit files, which are incorporated into a utility's existing network scanners and used to audit the control system's security settings against an optimal security configuration. Given that large control systems can have over 1000 security settings, Bandolier can help a utility enhance its security posture while

saving time and money at the same time. Audit files are now available for Siemens, Telvent, and ABB. Digital Bond has made its product available for a nominal subscriber fee on its website.

The Hallmark project, led by Schweitzer Engineering Laboratories (SEL), is another DOE-supported research and development project. SEL is working to commercialize the Secure SCADA Communications Protocol originally developed by Pacific Northwest National Laboratory. The technology will enable utilities to secure critical data communications links between remote substations and control centers and is scheduled to be launched in the next few months.

To track progress on implementation the Department designed a unique online collaborative tool – the interactive energy Roadmap (ieRoadmap) – which can be found online at www.controlsystemsroadmap.net. Public- and private-sector researchers self-populate the online database with project information and map their efforts to specific challenges and priorities identified in the Roadmap. The website has become a vital resource for news, information sharing, and collaboration.

Looking ahead, the Department also participates in multi-agency information-sharing forums such as the Networking and Information Technology Research and Development (NITRD) program, which is the primary mechanism for government to coordinate unclassified networking and information technology research and development investments. Thirteen Federal agencies are formal members (including DOE) of the NITRD Program.

Also in the long-term, the Department seeks to alter the very nature of cyber security. During the past two years, the Department's Office of Science has brought together a growing community of cyber security professionals and researchers from the laboratories, private industry, academia, and other government agencies to assess the state of cyber security in general and within the Department specifically. These experts concluded that the current approach to addressing cyber security problems is reactive and the Department should develop a long-term strategy that goes beyond stopping traditional threats to rendering both traditional and new threats harmless.

In December 2008, the Department released the findings of this group in "A Scientific Approach R&D Approach to Cyber Security," which outlines a set of opportunities to introduce anticipation and evasion capabilities to platforms and networks, data systems to actively contribute to their control and protection, and platform architectures that operate with integrity despite the presence of untrusted components. This approach could not only provide new, game-changing capabilities to the Department, but could also be directly applied to other agencies, industry, and society.

Smart Grid

The American Recovery and Reinvestment Act of 2009 appropriated $4.5 billion in funds for electricity delivery and energy reliability activities to modernize the electric grid, to include demand responsive equipment, enhance security and reliability of the energy infrastructure, energy storage, facilitate recovery from disruptions, and for implementation of programs authorized under Title XIII of the Energy Independence and Security Act of 2007 (Smart Grid).

The Department is working to implement these new program activities in a responsible manner and the request for proposals for these activities will include requirements that each applicant thoroughly and systematically addresses all cyber security risks to the system.

A key application of the smart grid is Advanced Metering Infrastructure (AMI). AMI requires two-way communication between the utility and the end-user. Over the last 10 months, DOE has partnered with the AMI Security (AMI-SEC) Task Force organized under the UCA International User's Group. The Task Force is comprised of utilities, security domain experts, standards body representatives and industry vendors. On March 10, 2009, the Task Force published the *AMI System Security Requirements***,** which provides critical guidance for vendors and utilities to help design and procure secure and reliable AMI systems. Because of the success of this industry-government collaboration, the Department is working with the Task Force to expand the activity to develop a suite of security requirements for all critical Smart Grid applications.

The National Institute of Standards and Technology (NIST) is responsible for developing the framework for interoperability standards development for the smart grid. The Federal Energy Regulatory Commission (FERC) has authority for issuing standards for rulemaking.

The Department views the development of interoperability standards that include appropriate cyber security protections as one of the key milestones toward realizing the goal of widespread implementation of smart grid technologies, tools, and techniques. DOE-NIST-FERC coordination on these standards has been ongoing for more than a year through the Federal Smart Grid Task Force, an EISA-mandated group that meets monthly and involves agencies from across the Federal government, including EPA, USDA, DHS, and DOD.

Recent progress on two key activities demonstrates the efficacy of the coordination effort: (1) Development of the Interoperability Standards Roadmap under the leadership of NIST, and (2) Development of a policy statement on interoperability standards under the leadership of FERC. These activities are critical for the Department in the selection of meritorious projects under the Smart Grid Investment Grants Program and the Smart Grid Regional Demonstration Program as the quality of the approaches for addressing interoperability and cyber security will be important evaluation criteria.

With regard to protecting the electric grid from newly discovered vulnerabilities, the Department does not have a position on the Draft Joint Staff Cybersecurity Text. The Department does provide the following technical comment:

> All vulnerabilities must be thoroughly evaluated on a scientific basis to determine the impact and risk to the nation in the event the vulnerability were to be exploited. Any decision to act or issue an order by the government must be based on sound risk management principals and judgment considering the characteristics of the vulnerability, the capabilities of the threat, likelihood of attack, the consequences to the nation should the vulnerability be exploited, and the cost of mitigation.

This concludes my statement, Mr. Chairman. Thank you for the opportunity to speak, and I look forward to answering any questions you and your colleagues may have.