STATEMENT OF
PATRICIA HOFFMAN
ACTING ASSISTANT SECRETARY
FOR ELECTRICITY DELIVERY AND ENERGY RELIABILITY
U.S. DEPARTMENT OF ENERGY

BEFORE THE
ENERGY AND COMMERCE COMMITTEE
ENERGY AND ENVIRONMENT SUBCOMMITTEE
UNITED STATES HOUSE OF REPRESENTATIVES
October 27, 2009

Thank you Chairman Markey and members of the Subcommittee for this opportunity to testify before you on emergency security directives and electric system reliability.

All of us here today have a common goal—ensuring the resiliency of the Nation's electric power grid. We all understand that vulnerabilities exist within the electric system and that the Department of Energy, in partnership with the rest of the Federal Government and power industry, should work towards implementing the "Roadmap to Secure Control Systems for the Energy Sector." [1]

The energy sector's threat analysis encompasses natural events, criminal acts, and insider threats, as well as foreign and domestic terrorism. Because of the diversity of assets and systems in the energy sector, a multitude of methodologies have been used to assess risks, vulnerabilities, and consequences.

Also to note, improving the resiliency of the Nation's electric power grid for the purpose of national security comes at a cost. New transformers can be electromagnetic pulse (EMP)-hardened for a very small fraction of the cost of the non-hardened item, e.g. one percent to three percent of cost, if hardening is done at the time the unit is designed and manufactured. In contrast, retrofitting existing functional components is potentially an order of magnitude more.[2] As Congress considers legislation, we recognize there are limited resources. Therefore we must prioritize based on risk, impact to the electric system and cost constraints.

---

[1] Department of Energy in collaboration with Department of Homeland Security and the Natural Resources Technology Directorate and the Energy Infrastructure Protection Division of Natural Resources Canada, 2006.

[2] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2004.

Vulnerabilities

The exploitation of high-risk vulnerabilities has become one of the greatest concerns for potential disruption. Control systems networks provide great efficiency and are widely used. However, they also present a security risk, if not adequately protected. Many of these networks were initially designed to maximize functionality and cost effectiveness, with little attention paid to security. With connections to the Internet, internal local area and wide area networks, wireless network devices, and modems, some networks are potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could cause disruptions to the Nation's critical infrastructure.

The United States Government is also considering the effect of High Impact-Low Frequency (HILF) events on our Nation's electric system. The Department is working with the North American Electric Reliability Corporation (NERC) to examine the effects of HILF events on the bulk power system. The effort will focus on HILF events such as influenza pandemic, space weather, terrorist attacks and electromagnetic pulses.

In addition, the Department, the Federal Energy Regulatory Commission (FERC), and the Department of Homeland Security (DHS), are funding an EMP study. The study will focus on electromagnetic threats and how they relate to the reliable operation of the U.S. electric power grid. The study will provide specific recommendations for activities to be accomplished in the future to achieve the protection of the U.S. electric power grid.

Incident response and information sharing still remain foremost concern. While the United States has a good deal of experience with physical disruptions to the grid, such as the 2003 Northeast Blackout and the Hurricanes of 2005 and 2008, it does not have experience-based lessons learned from a cyber incident. While coordination and communications have improved between public and private organizations over the past several years, much more is needed to prevent and respond to an attack that could hamper the U.S. electric power grid.

Enhancing the Security of the Energy Sector

For more than a decade, the Department has worked 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 and provided authorization to collaborate with all Federal agencies, state and local governments, and the private sector, to conduct

vulnerability assessments of the sector, and to encourage risk management strategies for critical energy infrastructure.

The Department takes this responsibility very seriously, and works closely with the private sector and state/Federal regulators to improve secure sharing of threat information and collaborate with the industry to identify and fund gaps in infrastructure research, development and testing efforts.

Our efforts to enhance the cyber security of the energy infrastructure have produced results in four areas. We have:

1. Identified cyber vulnerabilities in energy control systems and worked with vendors to develop hardened systems that mitigate the risks;
2. Developed more secure communications methods between energy control systems and field devices;
3. Developed tools and methods to help utilities assess their security posture; and
4. Provided extensive cyber security training for energy owners and operators to help them prevent, detect, and mitigate cyber penetration.

In 2003, the Department launched its National SCADA Test Bed (NSTB), a state-of-the-art national resource designed to aid government and industry in securing their control systems against cyber attack through vulnerability assessments, mitigation research, security training, and focused R&D efforts. The Department has expanded the NSTB to include resources and capabilities from five national laboratories.

To date, NSTB researchers have assessed the majority of SCADA/Energy Management Systems (SCADA/EMS) being offered in the energy sector. Twenty NSTB and on-site field assessments of common control systems from vendors including ABB, Areva, GE, OSI, Siemens, Telvent, and others, have led vendors to develop 11 hardened control system designs. Today, over 40 of these "hardened" SCADA/EMS systems have been deployed to better protect the power grid from cyber attacks, vendors have also issued many software patches to better secure legacy systems, which are now being used by 82 system applications in the sector. Findings from NSTB vulnerability assessments have also been generalized by Idaho National Laboratory into its *Common Vulnerabilities Report*, which includes mitigation strategies asset owners across the sector can use to better secure their systems.

The FY 2010 Energy and Water Appropriations Conference Report directs the Department to develop an independent national energy sector cyber security organization to institute research, development and deployment priorities,

including policies and protocols to ensure the effective deployment of tested and validated technology and software controls to protect the bulk power electric grid and integration of smart grid technology to enhance the security of the electricity grid. The Department recognizes the importance of an independent organization that includes industry in advancing cyber security and will make establishing this organization a top priority.

Cyber Security and the Smart Grid

Over the last 6 months, the Department has been highly focused on implementing several initiatives set forth in the Recovery Act, including $4.5B for smart grid activities designed to jumpstart the modernization of the electric power grid, reduce electricity use, reduce greenhouse gas emissions, and spur innovation and economic recovery. A key aspect for the implementation of smart grid technologies is the need to address interoperability and cyber security. It is paramount that smart grid devices and interoperability standards include protections against cyber intrusions and have systems that are designed from the start (not patches added on) that prevent unauthorized persons from gaining entry through the millions of new access points created by the deployment of smart grid technologies.

Under EISA Section 1305, Congress assigned the National Institute of Standards and Technology (NIST) with the responsibility to coordinate the development of a framework and roadmap for interoperability standards including cyber security. The Department has been working closely with NIST and other agencies through the Smart Grid Task Force and the private sector, and I am pleased to say significant progress has been made. NIST issued Release 1.0 of the "NIST Framework and Roadmap for Smart Grid Interoperability Standards" as well as Draft NISTIR 7628, "Smart Grid Cyber Security Strategy and Requirements." Recognizing the importance and urgency of cyber security standards for the Smart Grid, in May 2009 the Department partnered with the UCA International Users Group (UCAIug), Consumers Energy, Florida Power & Light, and Southern California Edison and launched the Advanced Security Acceleration Project - Smart Grid (ASAP-SG) specifically to accelerate the development of cyber security standards for the smart grid. ASAP-SG is developing a set of security profiles, each containing a baseline set of security controls for a given smart grid application. These profiles can be used by utilities and vendors to improve the security of smart grid applications and implementations. ASAP-SG is working closely with the NIST Cyber Security Coordination Task Group (CSCTG) and recently delivered an Advance Metering Infrastructure (AMI) security profile which is incorporated in the Draft NISTIR 7628.

Critical Infrastructure Protection and a Threat Analysis Methodology

In the aftermath of 9/11, we have strived to define and implement domestic threat policies that adequately balance the potential consequences associated with the loss/misuse of an asset; limited fiscal and physical resources; the capabilities of the intelligence community to identify threats in a timely manner; the ability of other agencies to interdict emerging threats; and the ability to effectively and quickly respond to constantly changing threats.

The Department recognized the inherent weaknesses associated with deriving system effectiveness and risk from a single "worst-case" scenario. A single "worst-case" scenario is possible, but rarely exists and often exceeds the known and projected adversary capabilities. At the same time, focusing on the "worst-case" scenario may result in overlooking protection system elements needed to counter more probable significant and credible threats. Consequently, the Department required a more balanced methodology to effectively detect and deter the threats.

Technical Comments on H.R 2195 and H.R. 2165

The Department reviewed the various bills and conducted analyses to evaluate effectiveness. We also reviewed existing cyber security standards and their relative effectiveness in addressing high consequence risks in a rapidly changing threat environment. The Department would like to provide the following technical comments:

The Federal Energy Regulatory Commission could be authorized to issue an Emergency Security Directive to owners and operators of the bulk power system, covering a specific period of time, if the Secretary of Energy has determined that a power grid emergency exists.

A "power grid emergency" is defined as a situation that poses a high risk to the bulk power system that must be addressed within 60 days without public disclosure. The determination of a power grid emergency would require the expertise of the Secretary of Energy, in consultation with the Secretary of Homeland Security, Office of Attorney General, and the Director of National Intelligence. In making a determination of a power grid emergency, the Secretary of Energy could consider the existence of the following conditions:

- A known cyber vulnerability exists that may affect the bulk power system.
- A threat actor is determined to have known or suspected intent, requisite resources, and capabilities to carry out the threat with a high likelihood.

- If exploited, the vulnerability would result in significant consequences, including damage to assets and infrastructure, loss of life, and psychological damage.
- The situation presents an imminent risk to the bulk power system.

Any directive should define security performance objectives and metrics for mitigating the identified threat, vulnerability, and/or potential consequences, and specify rules for satisfying the security performance objectives in accordance with the defined metrics within the defined time period of the power grid emergency and require that the fact of the Directive and its contents not be disclosed. The Directive may alternatively be in the form of an alert that notifies owners and operators of a potentially serious cyber situation without specifying mandatory actions that must be taken. Specific methods for compliance shall be left to the discretion of the provider of bulk electric power, provided the security performance objectives are met.

Any directive should notify private sector operators of the bulk power system of the nature of the risk, consistent with the proper handling of classified and restricted information, and direct the operators to investigate, take appropriate and corrective action, and report findings back to FERC within a specified time period, and, if required, direct owners and operators of the bulk power system, through NERC, to develop mitigations, to test and validate such mitigations, and to recommend corrective actions. The Department of Energy could provide technical support in the development, testing, and validation of such mitigation measures.

Conclusions

The scope and nature of security threats and their potential impact on our national security require the ability to act quickly to protect the bulk power system and to protect sensitive information from public disclosure. At the same time, we must continue to build long-term programs that improve information sharing and awareness between the public and private energy sector. The electric system is not the Internet. It is a carefully tended and balanced system that is critical to the Nation and the people. We must continue to strive towards an electric system that can survive an intentional cyber assault with no loss of critical functions.

The following are the Department's recommended courses of action:

- Continue implementation of the "Roadmap to Secure Control Systems for the Energy Sector."
- Study HILF events and conduct cost-benefit analyses of the mitigations

- Continue efforts to improve incident response and information sharing programs.
- As Smart Grid efforts are developed, build into such initiatives, security features designed to anticipate and address cyber security threats.

This concludes my statement Chairman Markey. Thank you for the opportunity to address the committee. I look forward to addressing any questions you or your colleagues may have.