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

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS, CYBER SECURITY AND SCIENCE AND TECHNOLOGY
COMMITTEE ON HOMELAND SECURITY
U.S. HOUSE OF REPRESENTATIVES

JULY 21, 2009

Thank you Chairwoman Clark and members of the Subcommittee for this opportunity to testify before you on electric sector vulnerabilities and cyber security issues.

All of us here today share a common concern that vulnerabilities exist within the electric system and that the Department of Energy, in partnership with the rest of the Federal Government and industry, should address the full spectrum of events, from high-impact, low-probability (HILP) to high-impact, high-probability. This is particularly true for smart grid systems, which by their very nature involve the use of information and communication technologies in areas and applications on the electric system where they have not been used before.

For more than a decade, the Department 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 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.

Securing critical infrastructure is a shared responsibility. Asset owners bear the main responsibility for ensuring that key resources are secure, for making the appropriate investments, for reporting threat information to the government, and for implementing protective practices and procedures. As the SSA, the Department works closely with the private sector and state/federal regulators to provide secure sharing of threat information and collaborates with industry to identify and fund gaps in infrastructure research, development and testing efforts.

With an economy in the process of recovering, it is even more critical that all energy sector stakeholders understand the available options, their associated costs, and the roadmap or path to a more secure energy infrastructure. As we deploy smart grid

technologies, load management technologies, plug-in hybrid electric vehicles and distributed generation/microgrids, we may find some measures may not become necessary, while new ones may emerge.

Critical Infrastructure Protection and Risk Management Framework

Since the energy sector is characterized by very diverse assets and systems, prioritization of sector assets and systems is highly dependent upon changing threats and consequences. The significance of many individual components in the network is highly variable, depending on location, time of day, day of the week, and season of the year.

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. No single methodology or tool has been used to assess risks to energy sector assets, such as the Nuclear Regulatory Commission's *design-basis threat* (DBT) which is used to design safeguards and systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. Lessons learned from DBT analysis in the nuclear industry could be applied to the electric industry especially for large generating stations, large substations and major control centers.

The exploitation of unintentional vulnerabilities has become one of the greatest concerns for potential disruption and high-consequence events. 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, 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 Department is planning to work with the Federal Energy Regulatory Commission and the North American Reliability Corporation (NERC) to examine the effects of HILP events on the bulk power system. The effort will focus on HILP events such as influenza pandemic, space weather, terrorist attacks and electromagnetic pulses. The purpose of this effort will be to develop a framework to look at causes and consequences and provide a tool to summarize preparedness, response, recovery and mitigation measures.

DOE does not have a program that would allow for private or publicly-owned utilities to receive Federal grants for hardening their equipment against an intentional or unintentional electromagnetic pulse.

Cyber Security - Information Sharing and Early Detection and Warning

The *Roadmap to Secure Control Systems in the Energy Sector (2006)* identified the need to improve information sharing between the government and the private sector as a high priority. In their 2008 Annual Report, the Energy Sector Control Systems Working Group (ESCWG), which has worked in partnership with the Department to implement the Roadmap, stated that most information protection and sharing issues between the U.S. Government and industry still have not been resolved.

The Department of Homeland Security (DHS) receives the most complete intelligence related to critical infrastructure protection because of its cross- sector responsibilities. DHS's Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) develops early intelligence warnings, which it shares with the Department. DHS alerts the US-Computer Emergency Readiness Team (US-CERT) and the North American Electric Reliability Corporation (NERC).

DOE does not have a separate alert system. DOE does, however, have mandatory reporting requirements for electric emergency incidents and disturbances (including cyber incidents) in the United States. Form OE-417, "Electric Emergency Incident and Disturbance Report," is used to alert DOE to electrical emergency incidents and disruptions within a one hour or six hour period depending on the type of emergency. This information allows the Department to quickly respond to energy emergencies that may impact the Nation's infrastructure. The information, collected from the electric power industry, helps DOE meet its overall national security and Federal Emergency Management Agency's National Response Framework responsibilities. DOE uses the data from this form to obtain situational awareness of energy emergencies of U.S. electric supply systems. DOE's Energy Information Administration (EIA) publishes the electric power emergency incidents and disturbances in its monthly EIA reports. The data may also be used to develop legislative recommendations, reports to Congress and as a basis for DOE investigations. When appropriate, information is shared with FERC.

Early intelligence warnings provide the industry and government some insight into a potential attack but may not allow for timely defense against many of them. Besides early intelligence warnings, the Department recommends that the industry develop its own capabilities for monitoring rogue, malicious behavior on their systems. The industry should monitor communications on their systems just as they monitor system performance. Diligence in upgrading security software and protocols are essential to minimizing the impact of these events.

One of the challenges in creating an effective information sharing system is how to share classified intelligence information with state agencies and utility operators not cleared to receive this information. The DHS has been working to grant clearances to appropriate members of the community. An additional difficulty is the means by which the information can be communicated. For example, a security chief at a Regional

Transmission Organization (RTO) may have a clearance, but not have any means of communication or storage to receive the classified information except through face-to-face communications.

Cyber Standards

Improving the security of the electric sector will require coordination and cooperation between regulatory agencies and industry. Because the security of the electric grid does not rely solely on voluntary private-sector measures, much work is being done to develop necessary cyber security standards. The Federal Energy Regulatory Commission through the NERC Critical Infrastructure Protection (CIP) has mandated standards CIP-002 through CIP-009 to provide a security framework for the identification and protection of critical cyber assets that support reliable operation. In addition, the International Electrotechnical Commission (IEC) Working Group 15 of Technical Committee 57 is developing IEC 62351, focusing on power systems control, data communications and security. The Power Engineering Society Substations workgroup is developing P1689, a trial use standard for retrofitting cyber security of serial Supervisory Control and Data Acquisition (SCADA) links in intelligent electronic devices for remote access. International Society of Automation security standard ISA99 addresses cyber security for control systems. The National Institute of Standards and Technology (NIST) is also developing specific recommendations and guidance for securing smart grid and other industrial control systems. It is clear that standards development is a priority, and this activity should be monitored closely for progress, implementation and gaps.

DOE Cyber R&D Program

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, researchers have assessed 90% of the current market offering of SCADA/Energy Management Systems (SCADA/EMS) in the electric sector, and 80% of the current

market offering in the oil and gas 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. Vendors have released countless 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.

In 2005, the Department, in cooperation with the DHS and Natural Resources Canada, worked directly with experts in the oil, gas, and electricity industries to develop a detailed, prioritized plan for cyber security improvements over the next 10 years, including best practices, new technology, and risk assessment. The results of this work were published in the 2006 *Roadmap to Secure Control Systems in the Energy Sector*, which lays out a vision 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 members defined goals, milestones, and priorities to guide the industry toward this vision.

Let me highlight two such projects that the Department is cost-sharing with the private sector to support the Roadmap:

- The Bandolier project, led by Digital Bond, is developing automated checklists of security configuration baselines, which, when deployed, can enable the audit of actual configuration settings against these baselines. Downloadable checklists have been developed and are now available for Siemens, Telvent, ABB, and SNC systems, and Digital Bond has worked to make its product available immediately and at a low cost to utilities by offering it as subscriber content on its website.
- The Hallmark project, led by Schweitzer Engineering Laboratories, is working to commercialize the Secure SCADA Communications Protocol originally developed by Pacific Northwest National Laboratory. The technology allows utilities to secure data communications between remote devices and control centers – a critical cyber access path. The technology will be available in a hardware device by mid-year.

The Department is also supporting research in academia through a multi-university R&D project entitled “Trustworthy Critical Infrastructure for the Power Grid (TCIP).” This project is led by the University of Illinois and includes Dartmouth College, Cornell University, Washington State University, and companies representing the spectrum of the electric power industry including utilities, vendors, regulatory bodies, control center operators, reliability coordinators, and market operators. TCIP is funded mainly by the National Science Foundation with supporting funds from the Department and the Department of Homeland Security, Science and Technology Directorate.

In addition to R&D and NSTB assessments, the Department supports extensive cyber security training to help asset owners learn security methods they can implement immediately to better secure their utilities. So far, the Department has trained more than 1,800 individuals in the energy sector and is also ramping up its new advanced Red Team/Blue Team training through Idaho National Laboratory. This week-long course invites asset owners to participate in a simulated attack scenario on an actual control systems environment, giving them hands-on attack and mitigation training.

In collaboration with the North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection Committee (CIPC), the Department leveraged its expertise and experience in cyber security assessments to develop foundational, intermediate, and advanced mitigations for the NERC "Top 10" vulnerabilities associated with control systems commonly used in the electric sector. The list was developed by NERC members including small, medium, and large entities across North America. The list is comprised of the most prevalent, most exploited, or highest consequence vulnerabilities that a typical utility might find in their facilities. Utilities are encouraged to use this list to augment their risk management processes. Utilities also used the list as means to select vendors and purchase systems that had security "built–in."

In addition to its R&D and partnership initiatives, the Department is working collaboratively with the private sector on several activities to ensure that cyber security is “baked in” to the Smart Grid. Over the past year, the Department has been working collaboratively with the Utilities Communications Architecture (UCA) Users Group (including utilities, vendors, et al) to develop cyber security requirements for advanced metering infrastructure (AMI) - a key application for the smart grid. The group produced a document titled “AMI System Security Specifications” which will help utilities procure secure AMI systems. The Department is now working to leverage this effort in cooperation with the UCA User Group to develop cyber security requirements for the full suite of smart grid technologies.

The Department is also working with the ESCSWG to update the 2006 Roadmap. The update will incorporate new information and lessons learned, update end states and milestones, and establish priorities that have come to the forefront since 2006, such as smart grid and wireless technologies. So far, the ESCSWG has identified gaps in the 2006 Roadmap, reviewed the Roadmap vision and goal structure, assessed changes in the control systems landscape, and collected ideas for implementation. In September 2009, the ESCSWG will bring together a broad section of asset owners and operators, researchers, technology developers, security specialists, and equipment vendors to establish new goals and prioritize control systems security needs in the energy sector. The ESCSWG plans to release the new roadmap in January 2010.

American Recovery and Reinvestment Act (ARRA) – Title XIII, Smart Grid

A smart grid uses information and communications technologies to improve the reliability, availability, and efficiency of the electric system. With smart grid, these

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.

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 principle, 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, are key distinguishing features of the smart grid compared to the existing system.

The Office of Electricity Delivery and Energy Reliability received $4.5 billion in the ARRA, of which about $3.4 billion is for grants for Smart Grid development and $615 million is for Smart Grid demonstrations. In order to gain the greatest return on investment, this grant money will be disbursed in six areas: equipment manufacturing, customer systems, advanced metering infrastructure, electric distribution systems, electric transmission systems, and integrated and/or crosscutting systems. The Federal funds for this program have been divided into two categories:

- Smaller projects in which the Federal share would be in the range of $300,000 to $20,000,000
- Larger projects in which the Federal cost share would be in the range of $20,000,000 to $200,000,000

Approximately 40% of Smart Grid Investment Grant (SGIG) funding will be allocated for smaller projects, while approximately 60% will be allocated for larger projects. DOE reserves the right to revise these allocations depending on the quantity and quality of the applications received.

DOE is working to reduce cyber security risks by including the following language in the grant announcement:

“Cyber security should be addressed in every phase of the engineering lifecycle of the project, including design and procurement, installation and commissioning, and the ability to provide ongoing maintenance and support. Cyber security solutions should be comprehensive and capable of being extended or upgraded in response to changes to the threat or technological environment. The technical approach to cyber security should include:

- A summary of the cyber security risks and how they will be mitigated at each stage of the lifecycle (focusing on vulnerabilities and impact).
- A summary of the cyber security criteria utilized for vendor and device selection.

- A summary of the relevant cyber security standards and/or best practices that will be followed.
- A summary of how the project will support emerging smart grid cyber security standards."

DOE intends to work with those selected for award, but may not make an award to an otherwise meritorious application if that applicant cannot provide reasonable assurance that their cyber security efforts will provide protection against broad based systemic failures in the electric grid in the event of a cyber security breach.

The following technical merit review criteria will be used in the evaluation of applications and in the determination of the SGIG project awards. The relative importance of the four criteria is provided in percentages in parentheses:

1. Adequacy of the Technical Approach for Enabling Smart Grid Functions (40%);
2. Adequacy of the Plan for Project Tasks, Schedule, Management, Qualifications, and Risks (25%);
3. Adequacy of the Technical Approach for Addressing Interoperability and Cyber Security (20%); and
4. Adequacy of the Plan for Data Collection and Analysis of Project Costs and Benefits (15%).

DOE's programs do not include grants to private or publicly-owned utilities for hardening their equipment against an intentional or unintentional electromagnetic pulse

Conclusion

The United States needs a comprehensive framework to ensure a coordinated response by the Federal, State, local and tribal governments, the private sector, and international allies to significant incidents related to the nation's electric power grid, particularly cyber. Implementation of this framework will require developing reporting thresholds, adaptable response and recovery plans, and the coordination, information sharing, and incident reporting mechanisms needed for those plans to succeed. The government, working with key stakeholders, should design an effective mechanism to achieve a true common operating picture that integrates information from the government and the private sector and serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions.

The focus should be on addressing the full range of threats and vulnerabilities to critical infrastructure versus the bulk power system and requires public-private and international partnerships.

Priority should be placed on deploying sensors for complete and greater depth in monitoring and diagnostics of physical and cyber events.

The Federal Government and industry must develop a security baseline and benchmark milestones for securing critical infrastructure.

As the capabilities of the threat continue to outpace our ability to develop and implement countermeasures, it is critical that control systems for critical applications be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical functions.

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