S. HRG. 112–40

CYBER SECURITY

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

TO

RECEIVE TESTIMONY ON A JOINT STAFF DISCUSSION DRAFT PERTAINING TO CYBER SECURITY OF THE BULK-POWER SYSTEM AND ELECTRIC INFRASTRUCTURE AND FOR OTHER PURPOSES

MAY 5, 2011

Printed for the use of the
Committee on Energy and Natural Resources

U.S. GOVERNMENT PRINTING OFFICE

67–362 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND NATURAL RESOURCES

JEFF BINGAMAN, New Mexico, *Chairman*

RON WYDEN, Oregon
TIM JOHNSON, South Dakota
MARY L. LANDRIEU, Louisiana
MARIA CANTWELL, Washington
BERNARD SANDERS, Vermont
DEBBIE STABENOW, Michigan
MARK UDALL, Colorado
JEANNE SHAHEEN, New Hampshire
AL FRANKEN, Minnesota
JOE MANCHIN, III, West Virginia
CHRISTOPHER A. COONS, Delaware

LISA MURKOWSKI, Alaska
RICHARD BURR, North Carolina
JOHN BARRASSO, Wyoming
JAMES E. RISCH, Idaho
MIKE LEE, Utah
RAND PAUL, Kentucky
DANIEL COATS, Indiana
ROB PORTMAN, Ohio
JOHN HOEVEN, North Dakota
BOB CORKER, Tennessee

ROBERT M. SIMON, *Staff Director*
SAM E. FOWLER, *Chief Counsel*
MCKIE CAMPBELL, *Republican Staff Director*
KAREN K. BILLUPS, *Republican Chief Counsel*

CONTENTS

STATEMENTS

APPENDIX

CYBER SECURITY

THURSDAY, MAY 5, 2011

U.S. SENATE,
COMMITTEE ON ENERGY AND NATURAL RESOURCES,
Washington, DC.

The committee met, pursuant to notice, at 9:37 a.m. in room SD–366, Dirksen Senate Office Building, Hon. Jeff Bingaman, chairman, presiding.

OPENING STATEMENT OF HON. JEFF BINGAMAN, U.S. SENATOR FROM NEW MEXICO

The CHAIRMAN. OK. Good morning. Thanks for coming today to this hearing. It's a hearing devoted to cyber security in the electric sector.

The safety of the North American power system is critical to the Nation's economy and to our security. Today that power system includes over 200,000 miles of high voltage transmission lines, thousands of generating facilities, millions of digital controls. Each year we upgrade and expand the system, adding more miles of transmission lines, new supply resources and control devices.

As we upgrade and expand the Nation's electric system we are also modernizing that system. Information technology and communication systems have come to play a significant role in ensuring the reliability and security of the electric sector. While modernization allows us to achieve a variety of important economic and environmental objectives, it also introduces new security concerns. As this process unfolds, preserving and enhancing the cyber security of our electric infrastructure must be among our top priorities.

So, let me highlight 2 things.

First, the electric sector is already subject to a set of mandatory and enforceable cyber security standards that are developed by industry stakeholders and approved by the Federal Energy Regulatory Commission. This fundamentally distinguishes the electric sector from virtually all other critical infrastructure sectors. However, I do not believe that the existing suite of reliability standards and the process for developing them is sufficient to defend electric infrastructure against deliberate cyber attacks and to address system vulnerabilities. The new authorities contemplated in the discussion draft that we've circulated fill these gaps in a way that will help to complement current cyber security standards.

The second point I wanted to make is that today it's almost 2 years since the day—since our cyber security hearing occurred in the 111th Congress. In fact, we are fortunate to welcome many of the same witnesses. The draft legislation we're discussing today is

very similar to the legislation we discussed in 2009. It recognizes positive changes in the standards development and approval processes.

However, in the time since our last hearing the security environment has also changed and certainly much more quickly. Cyber related threats can arise virtually anytime/anywhere and change without warning. For these reasons, there is no reason we should not delay in acting to enhance the cyber security of our electric system.

I note that this is not the only committee in the Senate working on cyber security issues. I welcome the opportunity to work closely with other committees to ensure that the product of this committee's efforts work seamlessly with the proposals coming out of other committee's work.

With that let me call on Senator Murkowski for her comments.

STATEMENT OF HON. LISA MURKOWSKI, U.S. SENATOR FROM ALASKA

Senator MURKOWSKI. Thank you, Mr. Chairman. Welcome to the witnesses this morning.

The 2007 Aurora experiment by the Department of Energy and the Idaho National Lab put us all on notice of dangers of a cyber attack. In that experiment researchers hacked into a replica power plant's control systems causing the generator to self destruct. Aurora showed us that large coordinated attacks could severely damage the Nation's electric infrastructure.

Since then there have been a growing number of cyber intrusions in government and critical infrastructure networks. Starting in November 2009, cyber attacks which were dubbed "Night Dragon" attacks, were launched against several global oil, energy and petrochemical companies. The attackers targeted highly sensitive proprietary and financing information on oil and gas fuel bids and operations. Then last year the Stuxnet worm demonstrated the complexity of what a potential cyber security attack could look like in this country.

I think we recognize that the danger that is posed to our Nation's electric infrastructure from a possible cyber attack is very clear. Congress must provide government agencies with the authority to respond to cyber security threats and their vulnerabilities and do so in a timely manner. At the same time it's critical to recognize the electric industry is currently the only critical infrastructure sector to have mandatory and enforceable cyber security standards in place. We must continue to encourage a public/private partnership to protect the Nation's critical infrastructure. To that end, we must ensure that the private sector has the information that it needs to respond to credible cyber threats and vulnerabilities.

I think we recognize that it is industry that has the expertise in operating our Nation's complex utility systems. The discussion draft legislation that we're considering can be part of a responsible solution. The draft provides both FERC and DOE with needed tools to address today's known risks and weaknesses as well as future threats.

We've also tried to respect the so-called section 215 process that was originally created in the 2005 Energy Policy Act. That Act

passed an electric reliability organization, since designated as NERC, with developing mandatory, enforceable, reliability standards in partnership with industry stakeholders. I understand that section of the discussion draft may still need a little bit of work here. So I would look forward to hearing from our witnesses on that aspect of it this morning.

One area that we have not included in the draft legislation are the physical threats posed by electromagnetic pulses and geomagnetic storms. Based on the testimony that we receive today the committee will need to decide if we should address those issues within this legislation. As the chairman has noted, this committee is just 1 of 7 committees that are examining the cyber issue. What we're considering today is an electricity sector piece. But it does appear that the administration and the leadership prefer a government wide, comprehensive approach to cyber security.

Clearly cyber security involves a great many actors and a host of technical considerations. We'll work to report out our part of the cyber puzzle. Then if a comprehensive approach is decided on, certainly work with other committees and leadership in fitting our piece into the broader field.

I thank you again, Mr. Chairman, and look forward to the testimony from the witnesses.

The CHAIRMAN. Thank you very much.

We have 5 witnesses today. Let me just introduce them briefly.

The Honorable Patricia Hoffman, who is the Assistant Secretary for the Office of Electricity Delivery and Energy in the Department of Energy. Thank you for being here.

Mr. Joseph McClelland, who is the Director of the Office of Energy Projects with the Federal Energy Regulatory Commission. Thank you for being here.

Mr. Gerry Cauley, who is President and Chief Executive Officer of the North American Electric Reliability Corporation. Thank you for being here.

Mr. David Owens, the Executive Vice President for Business Operations with Edison Electric Institute. Thank you for being here.

Finally, Mr. William Tedeschi, who is the Senior Scientist and Engineer with Sandia National Laboratory in Albuquerque.

Thank you all for coming. Why don't each of you take 5 or 6 minutes, tell us the main things you think we need to know about this subject? We will then have some questions.

Ms. Hoffman, please go right ahead.

STATEMENT OF PATRICIA HOFFMAN, ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, DEPARTMENT OF ENERGY

Ms. HOFFMAN. Good morning, Mr. Chairman and members of the committee. I'd like to extend my thanks to the chairman, the ranking member and the esteemed members of the committee for inviting me here today to discuss the cyber security issues facing the electric industry as well as the discussion draft legislation intended to strengthen the protection of the bulk power system and the electric infrastructure from cyber security threats. Ensuring a resilient electric grid is particularly important since it is arguably the most

complex and critical infrastructure, which other sectors depend upon for essential services.

The Homeland Security Presidential Directive 7 designated the Department as the sector specific agency for the energy sector. My office works closely with the private sector, and State and Federal regulators to provide secure sharing of threat information, to identify and fund gaps in infrastructure research and testing, to conduct vulnerability assessments, and to encourage risk management strategies for critical energy infrastructure. Our office is building its capabilities to facilitate assistance to industry, and to conduct forensics and obtain situational awareness.

The Administration's cyberspace Policy Review underscores the need to strengthen the public/private partnerships in order to design more secure technologies as well as improve the resilience of critical government and industry systems and networks. Our office has long recognized that neither the government, nor the private sector, nor individual citizens can meet cyber security challenges alone. We must work together.

The Office of Electricity Delivery and Energy Reliability (OE) has launched several new initiatives to enhance cyber security in the energy sector.

In coordination with the Department of Homeland Security and other Federal agencies, we have conducted several cyber threat information sharing workshops to analyze classified information to determine the impact to the sector and develop flexible mitigations specifically designed to work for the energy sector.

In coordination with National Institute of Standards and Technologies and NERC, OE is leading a collaborative effort with representatives from across the public and private sectors to develop cyber security risk management guidelines.

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. Some examples include: A technology to secure serial communications for control systems. Software tool kits that provide auditing of SCADA security settings. Vulnerabilities assessments of 38 different SCADA systems, and a common cyber security vulnerabilities report to help utilities and vendors mitigate vulnerabilities found in many SCADA systems. We are currently in the process of updating this report and hope to have that released this summer.

The Senate discussion draft recognizes the important difference between cyber security vulnerabilities and the cyber security threat. In addition, section 224F requires a comprehensive plan to identify emergency measures to protect the reliability of the electric power supply of national defense facilities. Pertinent to that, in July 2010 DOE and DOD signed a Memorandum of Understanding concerning cooperation and a strategic partnership to enhance energy security. This MOU will provide an opportunity to develop a comprehensive approach that reduces the impact of power loss to defense critical assets in considering both the mitigation and response measures to ensure vital defense capabilities are not disrupted.

Finally, the draft discussion does not address, a unique but sensitive cyber security information disclosure issue faced by the Federal Power Marketing Administrations that are subjected to both the Freedom of Information Act as well as mandatory reliability standards that are approved by FERC. This security vulnerability could be avoided if legislation was enacted that provided statutory protection of this information under Exemption Three of the Freedom of Information Act.

In conclusion, I would like to again thank this committee for its leadership in supporting the protection of the bulk power system and the 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 looks forward to the continued dialog with this committee on this legislation. I ask that my written statement be submitted for the record. I would be pleased to answer any questions this committee may have.

Thank you.

[The prepared statement of Ms. Hoffman follows:]

PREPARED STATEMENT OF PATRICIA HOFFMAN, ASSISTANT SECRETARY, OFFICE OF ELECTRICITY DELIVERY AND ENERGY RELIABILITY, DEPARTMENT OF ENERGY

Chairman Bingaman, Ranking Member Murkowski and members of the Committee, thank you for this opportunity to discuss the cyber security issues facing 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 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, 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.µDepartment 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 "Cyber Security Guidelines for the Smart Grid". 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.

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 identifies, defines, and distinguishes between a cyber security vulnerability and a cyber security threat. These are two related, but different concepts. Vulnerabilities need to be identified and addressed, while threats need to be protected against. 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 and mandatory reliability standards enacted under Section 215 of the Federal Power Act. This sensitive information, developed under the mandatory reliability standards, appears not to be protected from public disclosure under the Freedom of Information Act. This security vulnerability could be avoided if legislation providing statutory protection for this information were enacted that qualified under Exemption 3 of the Freedom of Information Act.

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.

The CHAIRMAN. Thank you very much. Everyone's statement will be included in the record as if read, including the one that you've prepared.

So, Mr. McClelland, go right ahead.

STATEMENT OF JOSEPH MCCLELLAND, DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION

Mr. MCCLELLAND. Mr. Chairman and members of the committee, thank you for the privilege to appear before you today to discuss the security of the power grid. My name is Joe McClelland and I am the Director of the Office of Electric Reliability at the Federal Energy Regulatory Commission. I am here today as a Commission Staff Witness and my remarks do not necessarily represent the views of the Commission or any individual commissioner.

In the Energy Policy Act of 2005 Congress entrusted the Commission with a major new responsibility, to oversee a mandatory, enforceable reliability and cyber security standards for the Nation's bulk power system. This authority is in section 215 of the Federal Power Act. It is important to note that FERC's authority under section 215 is limited to, "the bulk power system," which excludes Alaska and Hawaii, transmission facilities in certain large cities such as New York, as well as all local distribution systems.

Under section 215, FERC cannot author or modify reliability or cyber security standards but must depend upon an electric reliability organization or ERO to perform this task. The Commission selected the North American Electric Reliability Corporation or NERC as the ERO. The ERO develops and proposes cyber security

standards or modifications for the Commission's review which it can either approve or remand.

If the Commission approves the proposed cyber security standard it becomes mandatory and enforceable in the United States to all users, owners and operators of the bulk power system.

If the Commission remands a proposed standard it is sent back to the ERO for further consideration.

Pursuant to its responsibility to oversee the reliability and cyber security of the power grid, in January 2008 FERC approved eight cyber security standards known as the Critical Infrastructure Protection or CIP standards, but also directed NERC to make significant modifications to these standards. Compliance with these eight standards first became mandatory on July 1st, 2010. Although NERC has filed and the Commission has approved some modifications to the CIP standards the majority of the Commission's directed modifications to these standards have not yet been addressed by NERC. It is not clear how long it will take for the CIP standards to be modified to eliminate some of the significant gaps in protection within them.

On a related note, as Smart grid technology is added to the bulk power system greater cyber security protections will be required. Given that this technology provides more access points thereby increasing the grid's vulnerabilities. The CIP standards will apply to some but not most of the Smart grid applications. Moreover there are non cyber threats that also pose national security concerns. Naturally occurring events are physical attacks against the power grid that cause equal or greater disruption than cyber attacks and the Federal Government should have no less ability to protect against them.

One example is electromagnetic pulse or EMP. An EMP event could seriously degrade or shut down a large part of the electric power grid. In addition to manmade attacks, EMP events are also naturally generated caused by solar flares and storms disrupting the Earth's magnetic field.

Such events are inevitable, can be powerful and can also cause significant and prolonged disruptions to the power grid. In fact, FERC, DHS and DOE recently completed a joint EMP study conducted through the Oak Ridge National Laboratory. The study evaluated both manmade and naturally occurring EMP events to determine their effects on the power system and to identify protective mitigation measures that could be installed. Included among its findings was that without effective mitigation that the solar storm of 1921 which is considered a one in one hundred year event were to occur today, over 300 bulk power system transformers could be damaged or destroyed thereby interrupting power to 130 million people for 10 years.

Although section 215 of the Federal Power Act can provide an adequate statutory foundation for the development of routine reliability standards for the bulk power system, the threat of cyber attacks or other intentional, malicious acts against the grid is different. These are threats that can endanger national security that may be posed by criminal organizations, terrorist groups, foreign Nations or others, intent on attacking the United States through its electric grid. A widespread disruption of electric service can

quickly undermine our government, our military, our economy as well as endanger the health and safety of our citizens. Given the national security dimensions to this threat there may be a need to act quickly, to act in a manner where action is mandatory rather than voluntary and to protect certain information from public disclosure.

The Commission's legal authority is inadequate for such action. New legislation should address several key concerns.

First, FERC should be permitted to take direct action before a cyber or physical national security incident has occurred.

Second, FERC should be allowed to maintain the appropriate confidentiality of security sensitive information.

Third, the limitations on the term "bulk power system" should be understood as our current jurisdiction under 215 does not apply to Alaska and Hawaii as well as some transmission facilities and all local distribution facilities.

Fourth, entities should be able to recover costs they incurred to mitigate the vulnerabilities and threats.

Finally, legislation on national security threats to reliability should cover not only cyber security threats but also natural events and intentional, non-cyber, malicious acts including threats from an EMP.

The cyber security discussion draft addresses many of these issues. Thank you for your attention today. I look forward to any questions that you might have.

[The prepared statement of Mr. McClelland follows:]

PREPARED STATEMENT OF JOSEPH MCCLELLAND, DIRECTOR, OFFICE OF ELECTRIC RELIABILITY, FEDERAL ENERGY REGULATORY COMMISSION

Mr. Chairman and Members of the Committee: Thank you for this opportunity to appear before you to discuss the security of the electric grid. My name is Joseph McClelland. I am the Director of the Office of Electric Reliability (OER) of the Federal Energy Regulatory Commission (FERC or Commission). The Commission's role with respect to reliability is to help protect and improve the reliability of the Nation's bulk power system through effective regulatory oversight as established in the Energy Policy Act of 2005. I am here today as a Commission staff witness and my remarks do not necessarily represent the views of the Commission or any individual Commissioner.

My testimony summarizes the Commission's oversight of the reliability of the electric grid under section 215 of the Federal Power Act (FPA) and the Commission's implementation of that authority with respect to cyber security primarily through Order No. 706. I also will describe some of the current limitations in Federal authority to protect the grid against physical and cyber security threats, and also comment on the cyber security discussion draft. The Commission currently does not have sufficient authority to require effective protection of the grid against cyber or physical attacks. If adequate protection is to be provided, legislation is needed and my testimony discusses the key elements that should be included in legislation in this area.

BACKGROUND

In the Energy Policy Act of 2005 (EPAct 2005), Congress entrusted the Commission with a major new responsibility to oversee mandatory, enforceable reliability standards for the Nation's bulk power system (excluding Alaska and Hawaii). This authority is in section 215 of the Federal Power Act. Section 215 requires the Commission to select an Electric Reliability Organization (ERO) that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the Nation's bulk power system. The Commission has certified the North American Electric Reliability Corporation (NERC) as the ERO. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory

in the United States only after Commission approval. The ERO also is authorized to impose, after notice and opportunity for a hearing, penalties for violations of the reliability standards, subject to Commission review and approval. The ERO may delegate certain responsibilities to "Regional Entities," subject to Commission approval.

The Commission may approve proposed reliability standards or modifications to previously approved standards if it finds them "just, reasonable, not unduly discriminatory or preferential, and in the public interest." The Commission itself does not have authority to modify proposed standards. Rather, if the Commission disapproves a proposed standard or modification, section 215 requires the Commission to remand it to the ERO for further consideration. The Commission, upon its own motion or upon complaint, may direct the ERO to submit a proposed standard or modification on a specific matter but it does not have the authority to modify or author a standard and must depend upon the ERO to do so.

Limitations of Section 215 and the Term "Bulk Power System"

Currently, the Commission's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, and therefore excludes Alaska and Hawaii, including any federal installations located therein. The current interpretation of "bulk power system" also excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas. The Commission recently issued Order No. 743, which directs NERC to revise its interpretation of the bulk power system to eliminate inconsistencies across regions, eliminate the ambiguity created by the current discretion in NERC's definition of bulk electric system, provide a backstop review to ensure that any variations do not compromise reliability, and ensure that facilities that could significantly affect reliability are subject to mandatory rules. NERC is currently developing its response to that order. However, it is important to note that section 215 of the FPA excludes local distribution facilities from the Commission's reliability jurisdiction, so any revised bulk electric system definition developed by NERC will still not apply to local distribution facilities.

Critical Infrastructure Protection Reliability Standards

An important part of the Commission's current responsibility to oversee the development of reliability standards for the bulk power system involves cyber security. In August 2006, NERC submitted eight proposed cyber security standards, known as the Critical Infrastructure Protection (CIP) standards, to the Commission for approval under section 215. Critical infrastructure, as defined by NERC for purposes of the CIP standards, includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the "Bulk Electric System." Under NERC's implementation plan for the CIP standards, full compliance became mandatory on July 1, 2010.

On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards while concurrently directing NERC to develop significant modifications addressing specific concerns. The Commission set a deadline of July 1, 2009 for NERC to resolve certain issues in the CIP reliability standards, including deletion of the "reasonable business judgment" and "acceptance of risk" language in each of the standards. NERC concluded that this deadline would create a very compressed schedule for its stakeholder process. Therefore, it divided all of the changes directed by the Commission into phases, based on their complexity. NERC opted to resolve the simplest changes in the first phase, while putting off more complex changes for later versions.

NERC filed the first phase of the modifications to the CIP Reliability Standards (Version 2) on May 22, 2009. In this phase, NERC removed from the standards the terms "reasonable business judgment" and "acceptance of risk," added a requirement for a "single senior manager" responsible for CIP compliance, and made certain other administrative and clarifying changes. In a September 30, 2009 order, the Commission approved the Version 2 CIP standards and directed NERC to develop additional modifications to certain of them. Pursuant to the Commission's September 30, 2009 order, NERC submitted Version 3 of the CIP standards which revised Version 2 as directed. The Version 3 CIP standards became effective on October 1, 2010. This first phase of the modifications directed by the Commission in Order No. 706, which encompassed both Version 2 and Version 3, did not modify the critical asset identification process, a central concern in Order No. 706.

On February 10, 2011, NERC initiated the second phase of the Order No. 706 directed modification, filing a petition seeking approval of Version 4 of the CIP standards. Version 4 includes new proposed criteria to identify "critical assets" for pur-

poses of the CIP reliability standards. This filing is currently under review by the Commission. In order to better understand the NERC Version 4 petition, particularly the number of critical cyber assets that will be identified under this revision, the Commission issued data requests to NERC, with responses due on July 11, 2011, which reflects an extension of time requested by NERC.

The remaining CIP standards revisions to respond to the Commission's directives issued in Order No. 706 are still under development by NERC. It is important to note that the majority of the Order No. 706 directed modifications to the CIP standards have yet to be addressed by NERC. Until they are addressed, there are significant gaps in protection such as a needed requirement for a defense in depth posture. NERC's standards development plan filed with the Commission in April 2011 classifies these outstanding revisions to the CIP standards as "High Priority" with a targeted completion in the second quarter of 2012.

Identification of Critical Assets

As currently written, the CIP reliability standards allow utilities significant discretion to determine which of their facilities are "critical assets and the associated critical cyber assets," and therefore are subject to the requirements of the standards. In Order No. 706, the Commission directed NERC to revise the standards to require independent oversight of a utility's decisions by industry entities with a "wide-area view," such as reliability coordinators or the Regional Entities, subject to the review of the Commission. This revision to the standards, like all revisions, is subject to approval by the affected stakeholders in the standards development process. NERC has attempted to address this directive in Version 4 of the CIP standards, which is now under review by the Commission.

When, in Order No. 706, the Commission approved Version 1 of the CIP reliability standards, it also required entities under those standards to self-certify their compliance progress every six months. In December 2008, NERC conducted a self-certification study, asking each entity to report limited information on its critical assets and the associated critical cyber assets identified in compliance with reliability standard CIP-002-1. As the Commission stated in Order No. 706, the identification of critical assets is the cornerstone of the CIP standards. If that identification is not done well, the CIP standards will be ineffective at protecting the bulk power system. The results of NERC's self-certification request showed that only 29% of responding generation owners and operators identified at least one critical asset, while about 63% of the responding transmission owners identified at least one critical asset. NERC expressed its concern with these results in a letter to industry stakeholders dated April 7, 2009.

NERC conducted another self-certification survey of responsible entities to determine progress towards identification of critical cyber assets. It gathered information about critical assets and critical cyber assets as of December 31, 2009. This survey included additional questions designed to obtain a better understanding of the results from industry's critical asset identification process. In general, this survey did not demonstrate a significant increase in identified critical assets. NERC noted some encouraging results as well as some that were a cause for concern. In addition, the Regional Entities have been performing audits which have included registered entities' determination of their critical cyber asset lists. FERC staff has been observing selected audits to examine the Regional Entities' methods of conducting these audits. It is important to note that although "critical assets" are used to identify subsequent "critical cyber assets," only the subset of "critical cyber assets" are subject to the CIP standards.

NERC's Critical Infrastructure Protection Committee released a guidance document to assist registered entities in identifying their critical assets. That document, which took effect on September 17, 2009, provides "guidelines" that define which assets should be evaluated, provides risk-based evaluation guidance for determining critical assets, and describes reasonable bases that could be used to support that determination. A second NERC security guideline regarding critical cyber assets became effective on June 17, 2010. This security guideline "provides guidance for identifying Critical Cyber Assets by evaluating potential impacts to 'reliable operation' of a Critical Asset." Neither of these guidance documents contained any actions that were mandatory for users, owners or operators of the bulk-power system.

Version 4 of the CIP standards, which are currently pending before the Commission, would change the way in which critical assets are identified. Instead of using a loosely defined risk-based assessment methodology, CIP-002 Version 4 Attachment 1 contains what NERC describes as "uniform criteria for the identification of Critical Assets." For example, criterion 1.1 would identify generation plants equal to or greater than 1500MW as critical assets. The filing asserts that this would account for 29% of the installed generator capacity in the United States. Because this is an

on-going proceeding before the Commission, I am limited in what I can discuss about the merits of NERC's petition.

THE NERC PROCESS

As an initial matter, it is important to recognize how mandatory reliability standards are established. Under section 215, reliability standards must be developed by the ERO through an open, inclusive, and public process. The Commission can direct NERC to develop a reliability standard to address a particular reliability matter, including cyber security threats or vulnerabilities. However, the NERC process typically requires years to develop standards for the Commission's review. In fact, the CIP standards approved by the Commission in January 2008 took approximately three years to develop.

NERC's procedures for developing standards allow extensive opportunity for stakeholder comment, are open, and are generally based on the procedures of the American National Standards Institute. The NERC process is intended to develop consensus on both the need for, and the substance of, the proposed standard. Although inclusive, the process is relatively slow, open and unpredictable in its responsiveness to the Commission's directives. This process requires public disclosure regarding the reason for the proposed standard, the manner in which the standard will address the issues, and any subsequent comments and resulting modifications in the standards as the affected stakeholders review the material and provide comments. NERC-approved standards are then submitted to the Commission for its review.

The procedures used by NERC are appropriate for developing and approving routine reliability standards. The process allows extensive opportunities for industry and public comment. The public nature of the reliability standards development process can be a strength of the process. However, it can be an impediment when measures or actions need to be taken to address threats to national security quickly, effectively and in a manner that protects against the disclosure of security-sensitive information. The current procedures used under section 215 for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system, particularly in emergency situations. Certain circumstances, such as those involving national security, may require immediate action, while the reliability standard procedures take too long to implement efficient and timely corrective steps. On September 3, 2010, FERC approved a new reliability standards process manual filed by NERC. While this manual includes a process for developing a standard related to a confidential issue, the new process is untested and it is unclear how the process would be implemented.

FERC rules governing review and establishment of reliability standards allow the agency to direct the ERO to develop and propose reliability standards under an expedited schedule. For example, FERC could order the ERO to submit a reliability standard to address a reliability vulnerability within 60 days. Also, NERC's rules of procedure include a provision for approval of "urgent action" standards that can be completed within 60 days and which may be further expedited by a written finding by the NERC board of trustees that an extraordinary and immediate threat exists to bulk power system reliability or national security. However, it is not clear NERC could meet this schedule in practice. Moreover, faced with a national security threat to reliability, there may be a need to act decisively in hours or days, rather than weeks, months or years. That would not be feasible even under the urgent action process. In the meantime, the bulk power system would be left vulnerable to a known national security threat. Moreover, existing procedures, including the urgent action procedure, could widely publicize both the vulnerability and the proposed solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

In addition, a reliability standard submitted to the Commission by NERC may not be sufficient to address the identified vulnerability or threat. Since FERC may not directly modify a proposed reliability standard under section 215 and must either approve or remand it, FERC would have the choice of approving an inadequate standard and directing changes, which reinitiates a process that can take years, or rejecting the standard altogether. Under either approach, the bulk power system would remain vulnerable for a prolonged period.

This concern was highlighted in the Department of Energy Inspector General's January 2011 audit report on FERC's "Monitoring of Power Grid Cyber Security." The audit report identified concerns regarding the adequacy of the CIP standards and the implementation and schedule for the CIP standards, and concluded that these problems exist, in part, because the Commission's authority to ensure ade-

quate cyber security over the bulk electric system is limited. The audit report concludes that the Commission should take a more aggressive action when ordering new or revised standards and highlights its lack of authority to implement its own reliability standards or mandatory alerts in response to emerging threats or vulnerabilities. This report emphasizes the need for FERC to have additional authority for ensuring adequate cyber security over the bulk electric system.

Finally, the open and inclusive process required for standards development is not consistent with the need to protect security-sensitive information. For instance, a formal request for a new standard would normally detail the need for the standard as well as the proposed mitigation to address the issue, and the NERC-approved version of the standard would be filed with the Commission for review. This public information could help potential adversaries in planning attacks.

NERC's Formal Notices

Currently, the alternative to a mandatory reliability standard is for NERC to issue a formal notice encouraging utilities and others to take voluntary action to guard against a specific cyber or other vulnerability. Such a notice may be an Advisory, a Recommendation or an Essential Action. The notice approach allows for quicker action, but compliance with a notice is voluntary, and will likely produce inconsistent and potentially ineffective responses. For example, two Advisories and a Recommendation were issued in 2010 by NERC, regarding an identified cyber security threat referred to as "Stuxnet." The details of actions taken to mitigate the vulnerabilities identified by Stuxnet, and the assets to which they apply, as well as their effectiveness, are not known. Reliance on voluntary measures to protect national security is fundamentally inconsistent with the conclusion Congress reached during enactment of EPAct 2005, that voluntary standards are not sufficient to protect the reliability of the bulk power system.

SMART GRID

The need for vigilance will increase as new technologies are added to the bulk power system. For example, smart grid technology promises significant benefits in the use of electricity. These include the ability to better manage not only energy sources but also energy consumption. However, a smarter grid would permit two-way communication between the electric system and a large number of devices located outside of controlled utility environments, which will introduce many potential access points.

Smart grid applications will automate many decisions on the supply and use of electricity to increase efficiencies and ultimately to allow cost savings. Without adequate physical and cyber protections, however, this level of automation may allow adversaries to gain access to the rest of the company's data and control systems and cause significant harm. Security features must be an integral consideration when developing smart grid technology and must be assured before widespread installation of new equipment. The challenge will be to focus not only on general approaches but, importantly, on the details of specific technologies and the risks they may present.

Regarding data, there are multiple ways in which smart grid technologies may introduce new cyber vulnerabilities into the system. For example an attacker could gain access to a remote or intermediate smart grid device and change data values monitored or received from down-stream devices, and pass the incorrect data upstream to cause operators or automatic programs to take incorrect actions.

In regard to control systems, an attacker that gains access to the communication channels could order metering devices to disconnect customers, order previously shed load to come back on line prematurely, or order dispersed generation sources to turn off during periods when load is approaching generation capacity, causing instability and outages on the bulk power system. One of the potential capabilities of the smart grid is the ability to remotely disconnect service using advanced metering infrastructure (AMI). If insufficient security measures are implemented in a company's AMI application, an adversary may be able to access the AMI system and could conceivably disconnect every customer with an AMI device. If such an attack is widespread enough, the resultant disconnection of load on the distribution system could result in impacts to the bulk power system. If an adversary follows this disconnection event with a subsequent and targeted cyber attack against remote meters, the restoration of service could be greatly delayed.

In addition to any smart grid related standards that may be adopted by the Commission, the CIP standards will apply to some, but not most, smart grid applications. The standards require users, owners and operators of the bulk power system to protect cyber assets, including hardware, software and data, which would affect the reliability or operability of the bulk power system. These assets are identified

using a risk-based assessment methodology that identifies electric assets that are critical to the reliable operation of the bulk power system. If a smart grid device were to control a critical part of the bulk power system, it should be considered a critical cyber asset subject to the protection requirements of the CIP standards. However, this designation is currently up to the affected entity as part of its self-determination of critical cyber assets, as discussed previously.

Many of the smart grid applications will be deployed at the distribution and end-user level. For example, some applications may be targeted at improving market efficiency in ways that may not have a reliability impact on the bulk power system, such that the protection requirements of the CIP standards, as they are currently written, may not apply. However, as discussed above, these applications either individually or in the aggregate could affect the bulk power system.

PHYSICAL SECURITY AND OTHER THREATS TO RELIABILITY

The existing reliability standards do not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks and the Federal government should have no less ability to act to protect against such potential damage. One example of a physical threat is an electromagnetic pulse (EMP) event. In 2001, Congress established a commission to assess the threat from EMP, with particular attention to be paid to the nature and magnitude of high-altitude EMP threats to the United States; vulnerabilities of U.S. military and civilian infrastructure to such attack; capabilities to recover from an attack; and the feasibility and cost of protecting military and civilian infrastructure, including energy infrastructure. In 2004, the EMP commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack.[1] A second report was produced in 2008 that further investigated vulnerabilities of the Nation's infrastructure to EMP.[2] Both electrical equipment and control systems can be damaged by EMP.

An EMP may also be a naturally-occurring event caused by solar flares and storms disrupting the Earth's magnetic field. In 1859, a major solar storm occurred, causing auroral displays and significant shifts of the Earth's magnetic fields. As a result, telegraphs were rendered useless and several telegraph stations burned down. The impacts of that storm were muted because semiconductor technology did not exist at the time. Were the storm to happen today, according to an article in Scientific American, it could "severely damage satellites, disable radio communications, and cause continent-wide electrical black-outs that would require weeks or longer to recover from."[3] Although storms of this magnitude occur rarely, storms and flares of lesser intensity occur more frequently. Storms of about half the intensity of the 1859 storm occur every 50 years or so according to the authors of the Scientific American article, and the last such storm occurred in November 1960, leading to world-wide geomagnetic disturbances and radio outages. The power grid is particularly vulnerable to solar storms, as transformers are electrically grounded to the Earth and susceptible to damage from geomagnetically induced currents. The damage or destruction of numerous transformers across the country would result in reduced grid functionality and even prolonged power outages.

In March 2010, Oak Ridge National Laboratory (Oak Ridge) and their subcontractor Metatech released a study that explored the vulnerability of the electric grid to EMP-related events. This study was a joint effort contracted by FERC staff, the Department of Energy and the Department of Homeland Security and expanded on the information developed in other initiatives, including the EMP commission reports. The series of reports provided detailed technical background and outlined which sections of the power grid are most vulnerable, what equipment would be affected, and what damage could result. Protection concepts for each threat and additional methods for remediation were also included along with suggestions for mitigation. The results of the study support the general conclusion that EMP events pose substantial risk to equipment and operation of the Nation's power grid and under extreme conditions could result in major long term electrical outages. In fact, solar magnetic disturbances are inevitable with only the timing and magnitude subject to variability. The study assessed the 1921 solar storm, which has been termed a 1-in-100 year event, and applied it to today's power grid. The study concluded that

[1] Graham, Dr. William R. et al., Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (2004).

[2] Dr. John S., Jr. et al., Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (2008).

[3] Odenwald, Sten F. and Green, James L., Bracing the Satellite Infrastructure for a Solar Superstorm, Scientific American Magazine (Jul. 28, 2008).

such a storm could damage or destroy up to 300 bulk power system transformers interrupting service to 130 million people for a period of years.

The existing reliability standards do not address EMP vulnerabilities. Protecting the electric generation, transmission and distribution systems from severe damage due to an EMP-related event would involve vulnerability assessments at every level of electric infrastructure.

THE NEED FOR LEGISLATION

In my view, section 215 of the Federal Power Act provides an adequate statutory foundation for the ERO to develop most reliability standards for the bulk power system. However, the nature of a national security threat by entities intent on attacking the U.S. through vulnerabilities in its electric grid stands in stark contrast to other major reliability vulnerabilities that have caused regional blackouts and reliability failures in the past, such as vegetation management and protective relay maintenance practices. Widespread disruption of electric service can quickly undermine the U.S. government, its military, and the economy, as well as endanger the health and safety of millions of citizens. Given the national security dimension to this threat, there may be a need to act quickly to protect the grid, to act in a manner where action is mandatory rather than voluntary, and to protect certain information from public disclosure.

The Commission's current legal authority is inadequate for such action. This is true of both cyber and physical threats to the bulk power system that pose national security concerns.

Any new legislation should address several key concerns. First, to prevent a significant risk of disruption to the grid, legislation should allow the Commission to take action before a cyber or physical national security incident has occurred. In my opinion, the cyber security discussion draft addresses this concern by allowing the Commission to timely act on cyber security vulnerabilities before an incident occurs and by giving the Secretary of Energy emergency authority to act on cyber security threats. In particular, the Commission should be able to require mitigation even before or while NERC and its stakeholders develop a standard, when circumstances require urgent action.

Second, any legislation should allow the Commission to maintain appropriate confidentiality of sensitive information submitted, developed or issued under this authority. Without such confidentiality, the grid may be more vulnerable to attack and the Commission will not be able to adequately protect it. The cyber security discussion draft also includes provisions for protection of critical electric infrastructure information, which includes a provision for FERC to establish procedures to allow the Commission to release critical infrastructure information to the extent necessary to enable entities to implement any FERC order under the proposal. It also appropriately would require FERC to limit redistribution of information so that the information is only in the hands of those that need to know.

Third, if additional reliability authority is limited to the bulk power system, as that term is currently defined in the FPA, it would not authorize Commission action to mitigate cyber or other national security threats to reliability that involve certain critical facilities and major population areas. The cyber security discussion draft would apply to any entity that owns, controls, or operates critical electric infrastructure. While Alaska and Hawaii would be excluded, the discussion draft requires the Secretary of Defense to prepare a comprehensive plan to protect any national defense facilities located in those states.

Fourth, it is important that entities be able to recover costs they incur to mitigate vulnerabilities and threats. The cyber security discussion draft requires the Commission to permit public utilities to recover prudently incurred costs required to implement immediate actions ordered by the Secretary of Energy to avert or mitigate a cyber security threat. I support this provision and any clarifications that might better ensure recovery of costs incurred under this legislation.

Finally, in my view, any legislation on national security threats to reliability should address not only cyber security threats but also natural events; i.e., a geomagnetic disturbance, or intentional physical malicious acts (targeting, for example, critical substations and generating stations) including threats from an electromagnetic pulse. This additional authority would not displace other means of protecting the grid, such as action by federal, state and local law enforcement and the National Guard. If particular circumstances cause both FERC and other governmental authorities to require action by utilities, FERC would coordinate with other authorities as appropriate.

In short, any new authority should allow the Commission to quickly order mandatory measures that are focused and confidential to address fast-moving, sophisti-

cated and targeted cyber and physical attacks and natural events while providing cost recovery to the affected entities.

CONCLUSION

The Commission's current authority is not adequate to address cyber or other national security threats to the reliability of our transmission and power system. These types of threats pose an increasing risk to our Nation's electric grid, which undergirds our government and economy and helps ensure the health and welfare of our citizens. Congress should address this risk now. The cyber security discussion draft in front of us today would go a long way to resolving this issue. Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

The CHAIRMAN. Thank you very much.

Mr. Cauley, go right ahead.

STATEMENT OF GERRY CAULEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. CAULEY. Good morning, Chairman Bingaman, Ranking Member Murkowski, members of the committee and fellow panelists.

As CEO of the organization that is charged with overseeing the reliability and security of the North American grid, I wake up every day concerned about the emerging risks caused by intentional actions of our adversaries who would do harm to our Nation and to our citizens. The security of the North American power grid is an utmost priority for NERC. The mainstay of NERC's critical infrastructure program is a set of nine mandatory cyber security standards that we actively monitor and enforce.

We've recently made significant strides in improving our cyber standards. When I came onboard at NERC in 2010 I recognized the importance of establishing bright line criteria for the identification of critical assets to be protected. The new standard was developed in 6 months and filed with the Commission in February of this year and is pending their approval.

Our standards process works for what it was intended to do, to establish sustained, baseline requirements for the reliability and resilience of the bulk power system. However, there's no single approach, not even compliance with mandatory standards that will protect the grid against all threats from physical and cyber attacks. The threat environment is constantly changing and our defenses must keep pace. Achieving a high degree of resilience requires continuously adaptive measures beyond those outlined in our standards, measure we are actively pursuing today.

The most important of these activities is the operation of the electricity sector, information sharing and analysis center. In this role NERC works closely with Federal partners to promptly disseminate threat indications, warnings and analysis to electricity sector participants. The crux of a dynamic, adaptive strategy is to get timely, actionable information to the asset owners and operators and the experts in the field.

NERC staff has the necessary security clearances to work with the Department of Homeland Security, DOE and Federal intelligence agencies to generate unclassified recommendations that lead to actions by industry. Using this process NERC has issued 14 security related alerts since January 2010 covering such issues

as Aurora, Stuxnet, Night Dragon and other threats. The NERC alert system works well coupled with our CIP standards and availability of a new, confidential and expedited standards development process NERC has the tools we need to protect the cyber security of the bulk power system.

NERC is leading a number of other initiatives to ensure the resilience of the bulk power system.

We're preparing an industry wide security exercise in November 2011. Jointly with DOE and NIST, we are developing cyber security best practices for electric systems including distribution.

In collaboration with the DOE national labs, we're initiating a program to monitor grid cyber networks and another program to improve the training and qualifications of industry cyber experts.

With regard to the proposed draft legislation, first and foremost, NERC has consistently supported legislation to address cyber emergencies and improve information sharing between government and the private sector. It is my interpretation of section 215(d)(5) that FERC now has the authority to direct NERC to prepare a standard that is needed to address a specific vulnerability including cyber security and to do so by a certain date. Therefore it is not clear to me that the vulnerability section proposed in the new section 224(b) is needed.

If section 224(b) is returned, first I'm concerned that the jurisdiction extends to distribution systems which were intentionally excluded from jurisdiction of FERC and NERC in section 215. If the intent is to expand the scope of authority for electric system security into distribution systems this is a critical issue requiring involvement of the States and also calls for consultation with asset owners and operators and other stakeholders should be included in such a process.

Second, I'm concerned that no requirement exists in the draft legislation for FERC to identify any deficiency in existing reliability standards or a cyber security vulnerability for the ERO to address. Without some specific idea of the problem to be solved it would be difficult for the ERO to produce an adequate set of requirements.

Third, the discussion draft calls for the ERO to develop a reliability standard in response to a FERC order on vulnerabilities. But given the dynamic nature of threats and vulnerabilities many are not appropriate to be addressed by a standard. Currently NERC's essential action alerts are not legally enforceable. Legislation that provides a means for both standards and other emergency directives to be legally enforceable would significantly enhance the cyber security of the grid. Such an approach would require the involvement of both the ERO and the Commission and sufficient due process for those entities subject to the requirements.

I believe legislation addressing the security of the Nation's electricity infrastructure could be beneficial, that the framework should focus on enabling information sharing and problem solving between the government and private sectors. NERC's standards provide a baseline of cyber protection for a power grid. Our alert program is effective in addressing emerging threats. Legislation could help by addressing the due process requirements and enforceability of emergency directives.

Thank you for the opportunity to speak today. I look forward to your questions.

[The prepared statement of Mr. Cauley follows:]

PREPARED STATEMENT OF GERRY CAULEY, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

INTRODUCTION

Good morning Chairman Bingaman, Ranking Member Murkowski, members of the Committee and fellow panelists. My name is Gerry Cauley and I am the President and CEO of the North American Electric Reliability Corporation (NERC). I am a graduate of the U.S. Military Academy, a former officer in the U.S. Army Corps of Engineers, and have more than 30 years' experience in the bulk power system[1] industry, including service as a lead investigator of the August 2003 Northeast blackout and coordinator of the NERC Y2K program. I appreciate the opportunity to testify today on the discussion draft of cybersecurity legislation.

NERC's Mission

NERC's mission is to ensure the reliability of the bulk power system of North America and promote reliability excellence. NERC was founded in 1968 to develop voluntary standards for the owners and operators of the bulk power system. NERC is an independent corporation whose membership includes large and small electricity consumers, government representatives, municipalities, cooperatives, independent power producers, investor-owned utilities, independent transmission system operators and federal power marketing agencies such as TVA and Bonneville Power Administration.

In 2007, NERC was designated the Electric Reliability Organization (ERO) by the Federal Energy Regulatory Commission (FERC) in accordance with Section 215 of the Federal Power Act (FPA), enacted by the Energy Policy Act of 2005. Upon approval by FERC, NERC's reliability standards became mandatory within the United States. These mandatory reliability standards include Critical Infrastructure Protection (CIP) Standards 001 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States. Subject to FERC oversight, NERC and its Regional Entity partners enforce these standards, which are developed with substantial input from industry and approved by FERC, to accomplish our mission to ensure the reliability of the electric grid. In its position between industry and government, NERC embodies the often-invoked goal of creating effective partnerships between the public sector and the private sector.

As a result of society's growing dependence on electricity, the electric grid is one of the Nation's most critical infrastructures. The bulk power system in North America is one of the largest, most complex, and most robust systems ever created by mankind. Throughout North America, four interconnections with a capacity of over one-million megawatts of generation and nearly half-a-million miles of high voltage transmission lines all acting in unison, meet the electric needs of more than 340 million people, with a maximum demand of nearly 850 thousand megawatts. The electricity being used in this room right now is generated and transmitted in real time over a complex series of lines and stations from as far away as Ontario or Tennessee. As complex as it is, few machines are as robust as the bulk power system. Decades of experience with hurricanes, ice storms and other natural disasters, as well as mechanical breakdowns, vandalism and sabotage, have taught the electric industry how to build strong and reliable networks that generally withstand all but the worst natural and physical disasters while supporting affordable electric service. The knowledge that disturbances on the grid can impact operations thousands of miles away has influenced the electric industry culture of reliability, affecting how it plans, operates and protects the bulk power system.

THE CYBERSECURITY CHALLENGE FOR THE GRID AND NERC'S APPROACH TO ADDRESSING IT

Along with the rest of our economy, the electric industry has become increasingly dependent on digital technology to reduce costs, increase efficiency and maintain the

[1] The Bulk Power System (sometimes referred to as "BPS") is defined as generation and transmission of electricity greater than 100kv, in contrast to the distribution of electricity to homes and businesses at lower voltages.

reliability of the bulk power system. The networks and computer environments that make up this digital technology could be as vulnerable to malicious attacks and misuse as any other technology infrastructure. Much like the defense of this country, the defense of the bulk power system requires constant vigilance and expertise.

As CEO of the organization charged with overseeing the reliability and security of the North American grid, I am deeply concerned about the changing risk landscape from conventional risks, such as extreme weather and equipment failures, to new and emerging risks where we are left to imagine scenarios that might occur and prepare to avoid or mitigate the consequences. Some of those consequences could be much more severe than we have previously experienced. I am most concerned about coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures. These threats differ from conventional risks in that they result from intentional actions by adversaries and are not simply random failures or acts of nature.

The most effective approach against such adversaries is through thoughtful application of resiliency principles, as outlined in a National Infrastructure Advisory Council (NIAC) report on the grid delivered to the White House in October 2010. I served on that council along with a number of industry CEOs. Resiliency requires proactive readiness for whatever may come our way and includes robustness; the ability to minimize consequences in real-time; the ability to restore essential services; and the ability to adapt and learn. Examples of the NIAC team's recommendations include: 1) a national response plan that clarifies the roles and responsibilities between industry and government; 2) improved sharing of actionable information by government regarding threats and vulnerabilities; 3) cost recovery for security investments driven by national policy; and 4) a strategy on spare equipment with long lead times, such as electric power transformers.

CRITICAL INFRASTRUCTURE PROTECTION ("CIP") RELIABILITY STANDARDS AND OTHER NERC MEASURES TO ADDRESS CYBERSECURITY THREATS AND VULNERABILITIES

NERC's critical infrastructure program, including both reliability standards and alerts, provides many tools to respond to cyber threats and vulnerabilities. Industry, consumers, and government representatives all participate in the NERC standards development process and provide important expertise.

1. Reliability Standards

NERC has nine existing CIP standards that address the following areas:

- Standard CIP-001: Covers Sabotage Reporting.
- Standard CIP-002: Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System.
- Standard CIP-003: Requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.
- Standard CIP-004: Requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.
- Standard CIP-005: Requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.
- Standard CIP-006: Intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.
- Standard CIP-007: Requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).
- Standard CIP-008: Ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.
- Standard CIP-009: Ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

In December 2010, NERC approved an enhancement to its Critical Cyber Asset Identification standard (CIP-002 version 4) that establishes bright-line criteria for the identification of critical assets. This enhanced standard was filed with FERC in February 2011 and is currently pending FERC approval.

In addition to the development of reliability standards through NERC's regular processes, FERC has authorized NERC to use an expedited standards development process to meet urgent reliability issues. NERC also has rules approved by FERC to enable the development of special standards on an expedited, confidential basis to address imminent or longer term national security threats.

Finally, FERC can order NERC to develop a proposed reliability standard or a modification to a reliability standard to address a specific matter (such as a cyber threat or vulnerability) under FPA Section 215(d)(5). In addition, the NERC Board of Trustees may propose and adopt a standard in response to a FERC directive if the board determines that the regular standards process is not being sufficiently responsive to the Commission.

Compliance with the NERC CIP standards is an important threshold for properly securing the BPS. However, there is no single security asset, security technique, security procedure or security standard that, even if strictly followed or complied with, will protect an entity from all potential threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best-practices call for additional processes, procedures and technologies beyond those required by the CIP standards.

2. NERC Alerts

Not all vulnerabilities can or should be addressed through a reliability standard. In such cases, NERC Alerts are a key element in critical infrastructure protection. To address cyber challenges not covered under the CIP Standards, NERC works through its Electricity Sector-Information Sharing and Analysis Center (ES-ISAC) to inform the industry and recommend preventative actions.

NERC must be able to promptly disseminate threat indications, analyses and warnings to assist electricity-sector participants in taking protective actions. NERC staff with appropriate security clearances often work with cleared personnel from Federal agencies to communicate sanitized sensitive information to the industry. As defined in NERC's Rules of Procedure, the ES-ISAC developed the following three levels of Alerts for formal notice to industry regarding security issues:

- Industry Advisory.—Purely informational, intended to alert registered entities to issues or potential problems. A response to NERC is not necessary.
- Recommendation to Industry.—Recommends specific action be taken by registered entities. Requires a response from recipients as defined in the Alert.
- Essential Action.—Identifies actions deemed to be "essential" to bulk power system reliability and requires NERC Board of Trustees approval prior to issuance. Like recommendations, essential actions require recipients to respond as defined in the Alert.

The risk to the bulk power system determines selection of the appropriate Alert notification level. Generally, NERC distributes Alerts broadly to users, owners, and operators of the bulk power system in North America utilizing its Compliance Registry. Entities registered with NERC are required to provide and maintain up-to-date compliance and cyber security contacts. NERC also distributes the Alerts beyond the users, owners and operators of the bulk power system, to include other electricity industry participants who need the information. Alerts may also be targeted to groups of entities based on their NERC-registered functions (e.g.; Balancing Authorities, Planning Authorities, Generation Owners, etc.)

Alerts are developed with the strong partnership of Federal technical organizations, including the Department of Homeland Security and the Department of Energy National Laboratories, and bulk power system subject matter experts, called the HYDRA team by NERC. NERC has issued 14 CIP-related Alerts since January 2010 (12 Industry Advisories and two Recommendations to Industry). Those Alerts covered items such as Aurora, Stuxnet, Night Dragon and the reporting of suspicious activity. Responses to Alerts and mitigation efforts are identified and tracked, with follow-up provided to individual owners and operators and key stakeholders. In addition, NERC released one Joint Product CIP Awareness Bulletin in collaboration with DOE, DHS and the FBI titled, "Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)".

The NERC Alert system is working well. It is known by industry, handles confidential information and does so in an expedited manner. The information needed to develop the Alert is managed in a confidential and expedited manner and does not require a NERC balloting process.

NERC understands that the Congress is seeking to ensure the cybersecurity of the electricity grid. Using standards, Alerts and essential actions, NERC is already working with FERC and the industry to protect the cybersecurity of the bulk power system.

NERC WORK WITH DOD, DHS AND DOE TO PROTECT GRID CYBERSECURITY

As chair of the Electricity Sub-Sector Coordinating Council (ESCC), I work with industry CEOs and our partners within the government, including the Department of Defense, the Department of Homeland Security and the Department of Energy, to discuss and identify critical infrastructure protection concepts, processes and resources, as well as to facilitate information sharing about cyber vulnerabilities and threats. This type of public/private partnership is key to effective cybersecurity protection.

Recently, I met with officials from U.S. NORTHCOM where we discussed collaborating on various electric grid-focused activities including participation in the 2011 SecureGrid Exercise, providing electric sector situational awareness and collaborating on the Joint Capability Technology Demonstration (JCTD) Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS). The latter project is being proposed to understand how specific facilities could develop small reliable "micro-grids" on a short-term or emergency basis. Similarly, NERC is discussing a project with DOD to develop case studies at critical military installations to further understand the requirements for "flow of power" and the implications to military readiness.

NERC is working with DHS National Cybersecurity and Communications Integration Center to develop a Memorandum of Understanding for bi-directional sharing of critical infrastructure protection information between the government and the electricity sector in North America. NERC also provides leadership to two significant DHS-affiliated public-private partnerships. These are the Partnership for Critical Infrastructure Security (PCIS) and the Industrial Control Systems Joint Working Group (ICSJWG). The PCIS is the senior-most policy coordination group between public and private sector organizations. On the government side, PCIS comprises the National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) and the State, Local, and Tribal Government Coordinating Council (SLTGCC), as well as the chairs of all of the other Government Sector Coordinating Councils. On the private side, PCIS comprises the chairs of all of the private-sector coordinating councils. The ICSJWG is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, coordinated efforts on developing better vendor focus on security needs and cybersecurity policy issues.

NERC is engaged with DOE National Laboratories to further the level of awareness and expertise focused on cybersecurity, especially as it pertains to the bulk power system. We are working with Pacific Northwest National Laboratory on the Electric Sector Network Monitoring initiative and also on developing cybersecurity certification guidelines for Smart-Grid Cyber Operators. In a similar fashion, NERC is working with the Idaho National Laboratory to promote the Cyber Security Evaluation Tool for use within the electric sector. NERC also is partnering with the Industrial Control Systems Cyber Emergency Response Team to share threat, vulnerability and security incident information.

Finally, NERC is working with DOE and the National Institute of Standards and Technology to develop comprehensive cybersecurity risk management process guidelines for the entire electric grid, including both the bulk power system and distribution systems. We believe this to be particularly important with the increasing availability of smart-grid and smart-meter technologies. While the majority of technology associated with the smart grid is found within the distribution system, vulnerabilities realized within the distribution system could potentially impact the bulk power system. Everyone engaged in smart-grid and smart-meter implementation should ensure that appropriate security applications and technologies are built into the system to prevent the creation of additional threats and vulnerabilities.

NERC Comments on the Discussion Draft

First and foremost, NERC has consistently supported legislation authorizing some government entity to address cyber emergencies, as the draft would authorize the Secretary of Energy to do.

Second, NERC strongly supports any effort to improve information sharing between government and the private sector owners of critical electric infrastructure. NERC especially commends the provisions of the discussion draft directing the Secretary and the Commission to establish procedures on the release of critical infrastructure information to entities subject to the proposed legislation. NERC and the electric industry can only deal with the risks they are aware of. It is impractical, inefficient and impossible to defend against all possible threats or vulnerabilities. Entities must prioritize their resources to ensure they are protected against those risks that pose the greatest harm to their assets, their business and their cus-

tomers. The electric industry is in the best position to understand the impact that a particular event or incident could have on the bulk power system, but the industry does not have the same access to actionable intelligence and analysis that the government does. This lack of information leads the industry to be, at best, a step behind when it comes to protecting against potential threats and vulnerabilities. Too often the industry has heard from government agencies that the threats are real, but is given little or no additional information. This leads to frustration among the private sector leaders who are unable to respond effectively due to ill-defined and nebulous threat information.

NERC also appreciates the additional attention in the discussion draft to providing security clearances, but that route will not likely deal with the unavailability of actionable information for electricity industry decision-makers. NERC has over 1900 entities on its Compliance Registry, some have just a few employees and some have many thousands. It is important to be realistic about the number of clearances that may be made available. Of more importance is developing methods and procedures for sanitizing sensitive information so that it can usefully be made available to the broad range of private decision-makers who must take action to protect against the threat or vulnerability.

The bulk of NERC's comments are directed to the draft legislation's treatment of "Cyber Security Vulnerabilities," which are something less urgent than "Cyber Security Threats." NERC appreciates that the draft legislation proposes for the ERO to play a meaningful role in addressing cybersecurity vulnerabilities, as the ERO now does. As discussed above, NERC has the tools, the expertise and the relationships with government agencies, intelligence resources and industry subject matter experts to address identified vulnerabilities effectively and efficiently. FERC has the authority now under FPA Sec. 215(d)(5) to direct NERC to prepare a proposed standard to address a specific vulnerability or other matter, and to do so by a certain date. Thus, it is not clear to NERC that the vulnerability section (proposed new FPA Section 224(b)) is needed. If this section is retained, please consider the following concerns:

1. FERC's jurisdiction under this bill extends to distribution systems; the ERO's does not: The definition of Critical Electric Infrastructure in proposed Section 224 extends to distribution systems. Section 215 does not provide NERC with that jurisdiction. Thus, existing NERC reliability standards and requirements cannot be as broad as FERC's jurisdiction under the draft bill, and standards prepared by NERC at the direction of FERC similarly cannot be as broad as FERC's direction if FERC directs an action to protect the distribution system action. If NERC is intended to have the same jurisdiction as FERC over the distribution system and assets, this needs to be clarified. Without such clarification, FERC could always find that an ERO-proposed reliability standard "fails to provide adequate protection of critical electric infrastructure from a cybersecurity vulnerability" and reject the ERO's efforts under Section 224, effectively removing the ERO role from the vulnerabilities section.

2. Identification of vulnerability: No requirement exists in the legislation for FERC to identify any deficiency in existing reliability standards or the specific cybersecurity vulnerability for the ERO to address. Without some idea of the "target" that FERC would like the ERO to hit, it will be difficult for the ERO to produce an adequate set of requirements, assuming the jurisdiction issue above is addressed.

3. Enforceable tools in addition to standards: The discussion draft calls for the ERO to develop a reliability standard in response to a FERC order on vulnerabilities, but given the constantly changing nature of vulnerabilities, not all vulnerabilities can or should be addressed by a standard. Currently, NERC actions other than standards are not legally enforceable. Legislation that provides a means for both standards and other NERC directives to be legally enforceable would significantly enhance the cybersecurity of the grid. Such an approach would require the involvement of both the ERO and the Commission.

4. Due process: The discussion draft would authorize FERC to promulgate an interim final rule without consultation or any due process. In addition, unlike the 90-day sunset on DOE emergency orders, there is no such limitation on FERC interim final rules.

CONCLUSION

NERC works with multiple agencies, industry, consumers and government to support a coordinated comprehensive effort to address cybersecurity. As outlined today, NERC has many tools available including the ESCC and the ES-ISAC to address imminent and non-imminent threats and vulnerabilities through our Alerts and

standards processes. These existing processes should be enhanced, not pre-empted, by cybersecurity grid legislation.

We appreciate this opportunity to discuss NERC's activities on cybersecurity with the committee and to offer our views on legislation that would improve cybersecurity protection of the grid.

The CHAIRMAN. Thank you very much.

Mr. Owens.

STATEMENT OF DAVID K. OWENS, EXECUTIVE VICE PRESIDENT, BUSINESS OPERATIONS, EDISON ELECTRIC INSTITUTE

Mr. OWENS. Good morning, Chairman Bingaman, Ranking Member Murkowski and other distinguished members of this committee.

As was said earlier, my name is David K. Owens. I'm Executive Vice President at the Edison Electric Institute. You're aware that EEI is the trade association of the U.S. shareholder owned electric companies. Our members serve about 75–70 percent of end users of electricity. I certainly do appreciate this opportunity to appear before you today to talk about cyber security and critical electric infrastructure.

Now to accompany my written statement is a document titled, "Principles for Cyber Security and Critical Infrastructure Protection." Now this document was adopted by EEI's Board of Directors last September. It demonstrated the significant concern of our industry and our CEOs in particular, about cyber security threats and the need to develop consensus around a framework to improve security of the electric grid.

Now rather than me getting into all the details of observations I've made about the bill or restating my testimony. I'd like to leave you with 2 principle points.

I'd like to talk very specifically about the need for coordination, planning and information sharing. I believe some of the other witnesses, Secretary Hoffman stressed that. The need also for clear regulatory structure that focuses resources where they're needed.

Now all of you know cyber security is not a check the box exercise. You can't say if we do these ten things we're not going to have a cyber security problem. Instead cyber security requires an evolutionary process and an ongoing dialog involving industry and government. Now the threats that we face daily and the mechanisms for identifying them also vary. Sometimes a government will become aware of a threat or other times it will be the industry or individual utilities that will be aware of this or outside security firms or academia.

The point is that there is no perfect process for identifying what tomorrow's threats are nor how a creative hacker might exploit vulnerabilities. A better approach in my view is fostering coordination and dialogs both horizontally and vertically between industry and government. Now I know you're probably saying well what does he mean by that? Horizontal communication, in my view, is across—should be across the industry and across government.

Now the electric industry, the private sector, we're working with a lot of other utilities that serve our Nation. We're working with public entities. We're working with governmental entities and so forth because we all have a commonality of keeping the lights on.

So the entire electric sector is working very closely together. That's an example of horizontal communication.

We also have interdependencies. For example, we rely on telecommunications industry so that we can communicate and improve our overall day to day operations. We also use water systems in order to cool our facilities. We use transportation in order to move our fuel. We also look at financial markets that fund our operations. So there's an interdependency. That's also horizontal communication.

Now no single industry, in my view, can be considered secure unless we're engaged in coordination across those industry sectors. Let me talk a little bit about horizontal communication within the government. Here I'm perfectly sure that DOE and the FERC communicate regularly.

One agency probably has substantial intelligence about what's occurring in the electric network and in other vital facilities in our Nation, whereas the other agency may have the responsibility of mandating reliability standards. But it's critically important that those agencies work together. So in addressing cyber security, my view, is that the government needs to consider how they engage in horizontal communications as well.

Then there's vertical communications. The vertical communications is the government communicating with industry and vice versa. Now we are not in the business in the utility industry of identifying threats, but the government is and needs to coordinate very closely with industry. On the other hand, we're pretty good at operating our systems and providing reliable electric service and understanding how to address potential vulnerabilities.

So I believe there's a shared responsibility. There's a responsibility of government. There's a responsibility of industry to work together. If we're working together then we can provide greater security over the overall electric system.

One of the things that I've observed in terms of the disaster in Japan was the need for planning before a crisis occurs. Protecting critical infrastructure demands planning both from government and from the private sector. The roles and responsibilities need to be very clear. Now I applaud this committee's efforts and our Congress for its deep consideration of how we put these various pieces together to protect our critical infrastructure.

Let me move to my second principle. I'd like to believe that we all recognize that a risk based approach for dealing with cyber security that is identifying assets, that make the system vulnerable, is very, very critical. We strongly support that.

We also recognize as well that under section 215, the Federal Power Act, that we had mandatory and enforceable reliability standards. We recognize that. But we also recognize that there's a gap. That gap means that we need to have a process where we can deal with imminent threats. We have to separate imminent threats from potential vulnerabilities.

I see that I'm almost out of time. So I'm just going to say this. We look forward to work with the committee in these areas. I look forward to your questions.

[The prepared statement of Mr. Owens follows:]

PREPARED STATEMENT OF DAVID K. OWENS, EXECUTIVE VICE PRESIDENT, BUSINESS OPERATIONS, EDISON ELECTRIC INSTITUTE

My name is David Owens, and I am Executive Vice President in charge of the Business Operations Group at the Edison Electric Institute (EEI). EEI is the trade association of U.S. shareholder-owned electric companies and has international affiliate and industry associate members worldwide. EEI's U.S. members serve 95 percent of the ultimate customers in the shareholder-owned segment of the industry and represent about 70 percent of the U.S. electric power industry. I appreciate your invitation to discuss the cyber security of critical electric infrastructure and to comment on the Committee's draft legislation.

It is almost two years since I last had the opportunity to testify on this subject before this Committee. Since then, EEI's member companies—along with other owners, operators, and users of the electric grid—have continued to make cyber security a priority, while working together to make our critical infrastructure more resilient. In fact, EEI is part of a broader coalition of electric power stakeholders working on these issues. While I am not officially testifying on its behalf, this coalition includes several major trade associations representing the full scope of electric generation, transmission and distribution in the United States, as well as regulators, Canadian interests and large industrial consumers. Rarely do these groups find consensus on public policy issues, but in the case of securing the electric grid, there is unanimous support for a regime that leverages the strength of both the public and private sectors to improve cyber security. My testimony focuses on the value of this cooperative relationship, the unique nature of threats to the power grid, and the ongoing efforts of the nation's electric sector to respond to those threats.

I also will share our analysis of the Committee's bill, particularly as it relates to EEI's "Principles of Cyber Security and Critical Infrastructure Protection," which is attached for the record. This document was adopted by our Board of Directors last September in an effort to address cyber security threats and develop consensus around a framework to improve security for the electric grid. Included in this document, and most salient to the Committee's work today, are the following principles the industry believes are integral to successful cyber security policy:

- Leveraging public and private sector expertise, while including robust information sharing between government and the private sector, as well as among other stakeholders; and,
- A clear regulatory structure that focuses resources and attention on protecting truly critical assets from imminent threats.

PUBLIC-PRIVATE COORDINATION AND INFORMATION SHARING

Among the myriad lessons learned following the earthquakes and tsunami in Japan is the need for dialogue and coordination before disaster strikes. It is clear that critical infrastructure protection is a shared cause that demands planning, as well as an understanding of roles and responsibilities ahead of time.

Both the federal government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system. The optimal approach to utilizing the considerable knowledge of both government intelligence specialists and electric utilities in ensuring the cyber security of the nation's electric grid is to promote a regime that clearly defines these complementary roles and responsibilities and provides for ongoing consultation and sharing of information between government agencies and utilities.

Fundamentally, the private sector can be disadvantaged in assessing the degree and urgency of possible or perceived cyber threats because of limitations on its access to classified information. The government is entrusted with national security responsibilities and has access to volumes of intelligence to which electric utilities are not privy. Thus the government is able to detect threats, evaluate the likelihood or risk of a malicious attack, and utilize its expertise in law enforcement. On the other hand, electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and we understand how our complex systems are designed and operated. Owners, users, and operators of the electric grid are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such exploitation, including ensuring against unintended consequences of remedial actions. It is critically important to establish a workable structure that enables the government and the private sector to work together in order to provide a more secure system for our customers.

Thus, the industry appreciates that the Committee's draft bill acknowledges the need for intelligence sharing between government and the private sector, though we believe a more robust and explicit mandate is required.

It also is important to recognize that a strong industry partnership with government agencies currently exists. On an ongoing basis, the electric power industry communicates and collaborates in the United States with the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC). The industry also works very closely with the North American Electric Reliability Corporation (NERC) to develop mandatory reliability standards, including an array of "Critical Infrastructure Protection" or "CIP" standards. In addition, NERC, in its capacity as the Electric Sector Information Sharing and Analysis Center (ESISAC), uses its "alert and advisory" procedures to provide the electric power industry with timely and actionable information received from various federal agencies to assure the continued reliability and security of the nation's electric systems.

This NERC advisory system continues to evolve and, in the time since I last testified, has proven its ability to respond and disseminate information successfully when responding to significant national security events like the Stuxnet worm.

I would urge you not to reinvent the wheel, nor jump to conclusions about the efficacy of the existing cyber security regimes. The mechanisms in place to deal with these new and constantly evolving threats are, themselves, evolving. It is important that the Committee support continued participation in NERC's stakeholder-driven and FERC-approved standards and development process, which will yield mandatory CIP cyber security standards for the bulk power system that are clear, technically sound, and enforceable.

Finally, I would add that simply creating mechanisms for information sharing and public-private coordination is only part of the solution. Those lines of communication must be developed at the highest levels of both government and industry, and then drilled on a regular basis to ensure that, in times of crisis, those with relevant information and operational expertise can communicate seamlessly, quickly and, when needed, securely.

CLEAR, FOCUSED REGULATORY STRUCTURE

A successful cyber security framework also needs to focus on protecting truly critical assets from imminent threats. There is a security axiom that states: if you try to protect everything, you protect nothing. Put another way, risk-based prioritization ensures both government and private sector resources are allocated wisely.

The distinction between imminent threats and vulnerabilities is an important one. Threats, by definition, constitute an emergency, while vulnerabilities might be exploited at a later date, providing time to determine the best way to respond to them.

EEI agrees that it is appropriate for this Committee and Congress to consider legislation providing federal energy regulators new authority to address emergency cyber security threats. I want to emphasize, however, that current law already provides the means to address the many non-emergency cyber security issues in the electric industry. Section 215 of the Federal Power Act (FPA), which this Committee helped develop and which was enacted by Congress as part of the Energy Policy Act of 2005, provides for the Electric Reliability Organization to establish mandatory and enforceable electric reliability standards, specifically including standards to address cyber security, under FERC oversight. Chairman Bingaman and other Senators on this Committee should be commended for their work on enacting Section 215 and other efforts to ensure the reliability of the electric grid.

The basic construct of the relationship between FERC and NERC in developing and enforcing reliability standards is sound. In summary, NERC, using a well-defined stakeholder process that leverages the vast technical expertise of the owners, users, and operators of the North American electric grid, develops reliability standards, which are then submitted to FERC for review and approval. In approving such standards, FERC is to give "due weight" to the technical expertise of the ERO. Once approved by FERC, these standards are legally binding and enforceable in the United States. Any stakeholder, including FERC, may request that a standard be developed to address some aspect of reliability, expressly including cyber security.

I suggest the question on which the Committee should focus is, "What additional authority should be provided to federal energy regulators in order to promote clarity and focus in response to emergency situations?" Legislation in this area should complement, not supplant, the mandatory reliability regime already established under FPA Section 215. Any new federal authority should be appropriately narrow and focused only on unique problems that cannot be addressed under Section 215. The

Section 215 mandatory reliability framework reflects years of work and broad consensus reached by industry and other stakeholders in order to ensure a robust, reliable grid. It should not be undermined so early in its implementation.

While the open stakeholder processes used for developing industry-wide reliability and critical infrastructure protection standards admittedly are not well-suited to emergencies requiring immediate mandatory action with confidential handling of information, the vast majority of cyber security issues do not rise to the level of national security emergencies. Rather than creating broad new federal regulatory authorities that could undermine the consensus-driven policy framework developed through years of stakeholder input and memorialized in section 215, legislation should be focused on addressing a relatively narrow set of potential threats that legitimately merit special federal emergency authority.

Because of its extraordinary nature and potentially broad impacts on the electric system, any additional federal emergency authority in this area should be used judiciously. Legislation granting such authority should be narrowly crafted and limited to address circumstances where the President or his senior intelligence or national security advisors determine there is an imminent threat to national security or public welfare.

Also, the Committee draft provides DOE and FERC with parallel authorities to address cyber security threats and vulnerabilities, respectively. The Committee's draft could be clarified and strengthened by providing for a single agency to take expedited actions based on advice or information from the President or intelligence agencies.

To further focus efforts on those threats that have the potential to do the greatest harm, any new authority also should be limited to truly critical assets. Over-inclusion of electric utility infrastructure would be counterproductive; efforts to maintain and enhance the cyber security of the nation's critical electric infrastructure should focus first on the critical facilities that, if not protected, could cause substantial disruption to the nation's electric grid.

Any new legislation giving additional statutory authority should be limited to true emergency situations involving imminent cyber security threats where there is a significant declared national security or public welfare concern. In such an emergency, it is imperative that the government provide appropriate entities clear direction about actions to be taken, and assurance that those actions will not have significant adverse consequences to power operations or assets, while at the same time avoiding any possible confusion caused by potential conflicts or overlap with existing regulatory requirements.

BUILD SECURITY INTO THE GRID

A separate but equally important component of grid security is to ensure that manufacturers of critical grid equipment and systems are adequately fulfilling their security responsibilities by adopting good security practices in their organizations, building security into their products, and establishing effective programs so that, as new vulnerabilities are discovered, they can inform customers and provide technical assistance with mitigation. As grid technologies continue to evolve, they inevitably will include greater use of digital controls. Congress recognized the potential cyber security vulnerabilities, as well as benefits, that could result from greater digitization of the grid when it directed DOE to study these issues in Section 1309 of the Energy Independence and Security Act of 2007.

As new smart grid technologies are developed, it will be imperative for the industry to work closely with vendors and manufacturers to ensure they understand that cyber security is essential so that cyber security protections are incorporated into devices as much as possible.

EEI is encouraging the development of a security certification program and expansion of National Lab involvement to provide independent testing for new grid components. Such a program would help utilities differentiate among different vendor solutions to select those that provide appropriate cyber security.

FERC "INTERIM FINAL RULE" AUTHORITY

Under the Committee's draft legislation, FERC is to determine whether the current NERC reliability standards are "adequate to protect critical electric infrastructure from cyber security vulnerabilities." Under Section 224(b)(6)(C), any interim rule FERC enacts would stay in effect until NERC develops a reliability standard or modification that "the Commission determines provides adequate protection to critical electric infrastructure from the cyber security vulnerability addressed by the interim final rule."

Since NERC reliability rules apply only to the bulk electric system, FERC would have unilateral authority to write rules without input from the NERC stakeholder-driven process to establish technical standards. And, with no hearing or prior notice required before making the rule immediately effective, we are concerned about the lack of due process for stakeholder input. It would be desirable to at least have some requirement for FERC to consult with industry if time permits, similar to the consultation language in other parts of the bill.

FERC AND DOE EMERGENCY PROCEDURE AUTHORITIES

Having both FERC and DOE able to designate critical electric infrastructure introduces confusion and potential duplication. The lack of procedures or specific criteria for designating critical electric infrastructure is also problematic. It is unclear how, or if, an entity could challenge a designation by DOE under the general review provisions of the FPA.

CONCLUSION

With thousands of entities operating a single complicated, interdependent machine like the electric grid, the intra-industry coordination undertaken by the electric sector under the auspices of NERC has been invaluable.

There also are interdependencies not just within the electric sector, but across other critical infrastructure. For this reason, it would be preferable for Congress to take a comprehensive, multi-sector approach to legislation. Electric utilities, for example, rely on telecommunications systems to operate the grid, pipelines to fuel our generation, and wholesale markets to sell our product. Should any of these critical sectors be compromised, the electric grid would be impacted as well. The interconnected nature of critical infrastructure prevents us from claiming victory unless a comprehensive approach is taken. I understand this Committee's jurisdiction and interest focus specifically on protecting the electric grid, but would urge you to work with the appropriate congressional committees to address cyber security more holistically.

That said, while many cyber security issues already are addressed under current law, we believe it is appropriate to provide federal energy regulators with explicit statutory authority to address cyber security in a situation deemed sufficiently serious to require a Presidential declaration of emergency. In such a situation, the legislation should clarify the respective roles, responsibilities, and procedures of the federal government and the industry, including those for handling confidential information, to facilitate an expeditious response.

Promoting clearly defined roles and responsibilities, as well as ongoing consultation and sharing of information between government and the private sector, is the best approach to improving cyber security. Each cyber security situation requires careful, collaborative assessment and consultation regarding the potential consequences of complex threats, as well as mitigation and preventive measures, with owners, users, and operators of the bulk power system.

EEI and its member companies remain fully committed to working with the government and industry partners to increase cyber security. EEI's commitment to such coordinated efforts is illustrated by the broad coalition of industry stakeholder associations that continue to work together on these matters.

I appreciate the opportunity to appear today and would be happy to answer any questions.

ATTACHMENT.—EEI PRINCIPLES FOR CYBER SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

September 9, 2010

BACKGROUND

Protecting the nation's electric grid and ensuring a reliable supply of power is the electric power industry's top priority. Cyber security incidents may disrupt the flow of power or reduce the reliability of the electric system. Key to the success of this effort is the ability to provide measures capable of protecting the evolving intelligent network against interruption, exploitation, compromise or outright attack of cyber assets, whether the attack vector is physical, cyber or both.

The electric power industry takes cyber security threats very seriously. As part of the industry's overall reliability effort, electric companies work to maintain the reliability and the security of the computers, control systems, and other cyber assets that help electric companies operate the electric grid. In response to the cyber

threat, electric companies employ various strategies to protect these systems, but cyber security threats still exist.

ADDRESSING CYBER SECURITY THREATS

Reliability is more than a slogan for the electric utility industry—it's a mandate. In fact, federal and state regulators have significant interest and statutory authority in ensuring electric companies provide adequate reliability. Thus, utilities take very seriously their responsibility to address cyber vulnerabilities and the security of the computers, control systems, and other cyber assets that help operate the electric grid. This focus on reliability, resiliency and recovery takes into account an all-hazards approach, recognizing risks from natural phenomena such as hurricanes or geomagnetic disturbances to intentional cyber attacks.

Protecting the grid from cyber attacks requires a coordinated effort among electric companies, the federal government, and the suppliers of critical electric grid systems and components. Electric companies work closely with the North American Electric Reliability Corporation (NERC) and federal agencies to enhance the cyber security of the bulk power system. This includes coordination with the Federal Energy Regulatory Commission (FERC), the Department of Homeland Security (DHS), and the Department of Energy (DOE), as well as receiving assistance from federal intelligence and law enforcement agencies.

To complement its cyber security efforts and to address rapidly changing intelligence on evolving threats, the industry embraces a cooperative relationship with federal authorities to protect against situations that threaten national security or public welfare, and to prioritize the assets which need enhanced security. A well-practiced, public-private partnership utilizes all stakeholders' expertise, including the government's ability to provide clear direction and assess threats, while owners and operators of the critical infrastructure propose mitigation strategies that will avoid significant adverse consequences to utility operations or assets. At the same time a constructive regulatory environment will assure that incremental investments to protect the grid are prudent, and reduce risk in a manner proportional to the cost.

PROTECTING THE GRID IS A SHARED RESPONSIBILITY

1. Prioritize Assets to Ensure Effective Protection

Recognizing that there are a variety of interdependencies, and potential consequences associated with the loss of different facilities, the utility industry supports a risk-based, prioritized approach that identifies assets truly critical to the reliable operation of the electric grid. This ensures the most important elements of our system receive the highest level of attention, as well as the resources necessary to secure them.

2. Threats Require Emergency Action; Vulnerabilities Should Be Addressed More Deliberately

In this context, a threat is imminent and requires a rapid response. In these instances, the industry is willing to accommodate certain operational consequences in the interest of addressing the threat. Vulnerabilities, on the other hand, have a longer time horizon and can benefit from a more measured response. Government authority should reflect and respect these different levels of danger.

3. Clear Regulatory Structure and Open Lines of Communication

The Federal regulatory framework and roles for all stakeholders involved in securing the electric grid should be clear to avoid duplicative or conflicting actions in times of crisis. The electric utility industry is not in the law enforcement or intelligence gathering business, and the government has limited experience operating the electric grid. Thus, each should be consulted, and the flow of information should be regularly exercised, before a threat becomes a crisis. It is critical that the federal government and industry communicate with each other seamlessly; to avoid confusion, those at the highest levels of government and industry should be involved in coordinating responses and declaring the need for emergency action.

4. Proactively Manage New Risks

As the new Smart Grid develops, it is essential that cyber security protections are incorporated into both the grid architecture and the new smart grid technologies. The electric power industry must continue to work closely with vendors, manufacturers, and government agencies and be aligned with emerging and evolving cyber security standards (such as those being driven by NIST) to ensure that the new technology running the grid is, most importantly, secure and reliable. We encourage the development of a security certification program that would independently test

smart grid components and systems and certify that they pass security tests. This certification process would help utilities select only those systems that provide appropriate cyber security.

5. Committed to Protecting Bulk Electric System and Distribution Assets

The utility industry understands that cyber attacks affecting distribution systems could have broader implications. Since jurisdiction is split between state regulators and the Federal Energy Regulatory Commission, the utility industry supports enhanced threat information coordination and communication between regulatory agencies and utilities to protect our systems (whether distribution or the bulk electric system) while also honoring the existing regulatory model.

6. Cost Recovery and Liability Protection

Costs associated with emergency mitigation are, by definition, unexpected and thus not included in a utility's rate base. To ensure emergency actions do not put undue financial strain on electric utilities, the industry supports mechanisms for recovering costs. In addition, electric utilities support liability protections for actions taken under an emergency order.

The CHAIRMAN. Thank you very much.

Mr. Tedeschi, go right ahead.

STATEMENT OF WILLIAM TEDESCHI, SENIOR SCIENTIST, SANDIA NATIONAL LABORATORIES, ALBUQUERQUE, NM

Mr. TEDESCHI. Good morning, Chairman Bingaman, Ranking Member Murkowski and distinguished members of the Senate Committee on Energy and Natural Resources. Thank you for the opportunity to testify. I am William Tedeschi, Senior Scientist and Licensed Professional Engineer at Sandia National Laboratories, a multi program, national security laboratory. I am honored to be here today with the Honorable Patricia Hoffman of the United States Department of Energy, Joe McClelland of the Federal Energy Regulatory Commission, Gerry Cauley of the North American Electric Reliability Corporation and David Owens of the Edison Electric Institute.

Sandia is one of the 3 national Nuclear Security Administration Laboratories with responsibility for stockpile stewardship and annual assessment of the Nation's nuclear weapons. Within the U.S. nuclear weapons complex, Sandia is uniquely responsible for the systems engineering and integration of the nuclear weapons and the stockpile and for the design development and qualification of non-nuclear components of nuclear weapons. While nuclear weapons remain Sandia's core mission the science and technology and engineering capabilities required to support this mission position us to support other aspects of national security as well. Indeed there is natural increasingly significant synergy between our core mission and our broader national security work.

This broader role involves research and development and nonproliferation, counter proliferation, counter terrorism, energy security, defense and homeland security. My statement today will focus on the risk of nuclear electromagnetic pulse threats against the U.S. power grid and the potential need to harden the grid against such threats. I am a subject matter expert, nuclear weapons system and affects including electromagnetic pulse threats and in assessing the risks posed by such threats.

I will first refer to the results of a recent technical peer review of 7 reports focused on the topic of this testimony, a peer review that a Sandia team of experts provided to the Federal Energy Regulatory Commission.

Then I will present the view of the Sandia team on the risk of nuclear electromagnetic pulse attacks and the potential need to harden the U.S. power grid against them.

We commend the Federal Energy Regulatory Commission and the authors of the 7 reports on evaluating the impact of nuclear, high altitude, EMP pulse threats to the U.S. power grid for their comprehensive work which represents an excellent start on modeling a very complex problem. However we respectfully suggest that further computational and experimental work is required before fully informed decisions can be made about where and to what extent the power grid should be hardened solely against nuclear, high altitude, electromagnetic pulse threats. If the decision is made to protect the power grid against a broader set of more likely electromagnetic pulse threats including solar geomagnetic and electromagnetic interference threats than an awareness of nuclear, high altitude, EMP environments in effect, should also be considered.

From an integrated risk perspective the Sandia team considers nuclear, high altitude, electromagnetic pulse threats to be a remote likelihood. Also, the true extent of the grid's susceptibility and vulnerability to such effects and the resulting consequences are mostly unknown. Except for the apparent worse case environments and assumptions made in the reports that the Sandia team, peer review, evaluated.

The Sandia team recommends that this complex problem be studied in more depth in order to include results from additional computer based simulations and experimental testing specifically under nuclear, high altitude, electromagnetic threat conditions.

How to high voltage transformers and their protection and control elements respond to the range of induced current insults?

If they fail, how do they fail and at what level of insult?

Answering such questions would provide critical data to enable better understanding and validation of results by advancing a complete understanding of all the risk elements as well as quantification and reduction of uncertainties in order to fully inform decisions that may be made about hardening the U.S. power grid.

We suggest that a graded hardening approach to be considered whereby selective hardening could be accomplished easily and cost effectively in combination with addressing new and emerging threats to the grid, for example intentional electromagnetic interference. Also by further evaluating the consequence of electromagnetic pulse attacks on mission critical U.S. installations and functions, for example important U.S. war fighting or continuity of operations. Specific sites may be identified that may require selective electromagnetic pulse hardening.

This concludes my prepared remarks. I would be pleased to respond to any questions. Thank you.

[The prepared statement of Mr. Tedeschi follows:]

PREPARED STATEMENT OF WILLIAM TEDESCHI, SENIOR SCIENTIST, SANDIA NATIONAL LABORATORIES, ALBUQUERQUE, NM

INTRODUCTION

Chairman Bingaman, Ranking Member Murkowski, and distinguished members of the Senate Committee on Energy and Natural Resources, thank you for the opportunity to testify. I am William Tedeschi, senior scientist and licensed professional engineer at Sandia National Laboratories. Sandia is a multiprogram national secu-

rity laboratory owned by the United States Government and operated by Sandia Corporation[1] for the National Nuclear Security Administration (NNSA).

Sandia is one of the three NNSA laboratories with responsibility for stockpile stewardship and annual assessment of the nation's nuclear weapons. Within the U.S. nuclear weapons complex, Sandia is uniquely responsible for the systems engineering and integration of the nuclear weapons in the stockpile and for the design, development, and qualification of nonnuclear components of nuclear weapons. While nuclear weapons remain Sandia's core mission, the science, technology, and engineering capabilities required to support this mission position us to support other aspects of national security as well. Indeed, there is natural, increasingly significant synergy between our core mission and our broader national security work. This broader role involves research and development in nonproliferation, counterproliferation, counterterrorism, energy security, defense, and homeland security.

My statement today will focus on the risk of nuclear electromagnetic-pulse (EMP) threats against the U.S. power grid and the potential need to harden the grid against such threats. I have been employed at Sandia National Laboratories for 26 years, where I have done engineering work on the U.S. nuclear stockpile and have assessed a broad range of foreign threats to U.S. national security assets and infrastructures. I am a subject matter expert in nuclear weapon systems and effects, including EMP threats, and in assessing the risks posed by such threats. Part of this expertise came from Sandia having technically supported the congressionally mandated EMP Commission from 2002 to 2008 through targeted EMP testing of a whole range of electronic equipment, assessments of water-and financial-system infrastructure susceptibility, and targeted writing assignments. I was the program manager for that work. My testimony starts with a description of a recent technical peer review of seven reports focused on the topic of this testimony, a peer review that a Sandia team of experts provided to the Federal Energy Regulatory Commission; thereafter, the testimony puts forward the view of the Sandia team on the risk of EMP attacks and the potential need to harden the U.S. power grid against them.

MAJOR POINTS OF THIS TESTIMONY

It is the belief of a Sandia team of experts that

1. Nuclear high-altitude electromagnetic-pulse (HEMP) attacks against the U.S. power grid are of remote likelihood.
2. The susceptibility of the power grid to EMP attacks is not well characterized and should be further addressed with computer-based simulations and experimental testing in order to understand all the risk elements, quantify and reduce uncertainties, and thus fully inform decisions that may be made about the U.S. power grid.
3. Possible approaches to mitigating electromagnetic threats to the U.S. power grid could be graded hardening, whereby selective hardening would be accomplished easily and cost-effectively while addressing new and emerging threats to the grid, or selective hardening for protection of some critically important U.S. nodes.

ELECTROMAGNETIC PULSE (EMP) THREATS TO THE U.S. POWER GRID

Sandia Team Provided a Technical Peer Review for the Federal Energy Regulatory Commission

The Federal Energy Regulatory Commission (FERC) recently requested Sandia to do a peer review of seven reports (more than 700 pages in length) on electromagnetic threats to the U.S. power grid and on possible actions for mitigating such threats. A team of six subject matter experts (including myself) in EMP threats and effects, including damage susceptibility and consequences, conducted this work. Included in the team were two members with significant expertise in modeling national infrastructures and their interdependencies. Our assessment and recommendations do not constitute a position of or an endorsement by Sandia National Laboratories. Rather, they represent the conclusions the team reached after conducting a technical service Sandia is frequently called upon to perform for national security purposes. The team's high-level observations and findings were threefold:

- The reports are comprehensive, and the authors' knowledge about the U.S. power grid design and operations, as well as solar-induced and nuclear high-altitude EMP (HEMP) environments, is impressive.

[1] Sandia Corporation is a subsidiary of the Lockheed Martin Corporation under Department of Energy prime contract no. DE-AC04-94AL85000.

- The work represents an excellent start on modeling a very complex problem, but it is not yet complete and, in our view, should not be the basis for any short-term national decisions on whether and to what extent to harden the U.S. power grid solely against nuclear HEMP threats.
- Further study of this complex problem is recommended in order to include computer-based simulations and experimental testing to better understand, validate, and add to the existing work so that a complete understanding of all the risk factors and associated uncertainties can be obtained to support ongoing decisions.

Some additional general comments about the reports that the Sandia technical peer review team provided to FERC include the following:

The identified threats appear to be worst-case nuclear HEMP threats, but no details are provided to indicate the seriousness and plausibility of such threats or what might be the full spectrum of possible HEMP threats. Not all nuclear bombs are created equal; technical details matter—details not only on the potential severity of nuclear HEMP effects, but also on the likelihood of such threats ever materializing. Further elaboration on this aspect is warranted but must be done in a classified setting.

Numerous assumptions are made about the nuclear HEMP environments' coupling efficiency into the exposed power grid and about the susceptibility of key system elements and the upset or damage that might occur to those key elements (that is, protective features, control systems, and the high-voltage transformers). Few to no data and only a few referenced citations and limited technical analysis are offered to buttress the assertions made. Many assumptions are also made about the power grid and the type and implementation of its equipment. The power grid referenced in the reports as the "normal grid design" is portrayed without any information about validation from utilities. Assumptions about age, design, and failure thresholds of transformers introduce additional uncertainty and are based on limited samplings of transformers of a particular type and from a clear source. All the assumptions point to large uncertainties in the output results and interpretations from the model; therefore, statements on the number of "at-risk" transformers and the severity of the regional damage should be viewed as illustrative only. More modeling and simulation and experiments to characterize the response space of these key elements are recommended.

Finally, in our team's view, the reports' assessment of possible effects on the U.S. power grid as a result of nuclear HEMP attacks is too negative, based on a series of compounded, apparently worst-case assumptions. The reports lack discussion of the effect of possible uncertainties and mitigators on the results.

More detailed and specific technical comments were submitted to FERC for its consideration, and those can be provided upon request.

SANDIA TEAM'S POSITION ON ELECTROMAGNETIC PULSE (EMP) THREATS TO THE U.S. POWER GRID

Background on Nuclear High-Altitude EMP (HEMP) Threats: Effects, Damage, and Hardening

Nuclear EMP effects at Earth's surface are created by nuclear bomb explosions high inside the atmosphere (at an altitude of 40?100 kilometers) and in near outer space (from 100 kilometers to hundreds of kilometers above Earth's surface). According to publicly available information, both the United States and Russia experienced and characterized this class of nuclear weapon effects in the early 1960s during their high-altitude nuclear tests. The type and yield of the bomb and the altitude at which it is detonated primarily determine the strength of the EMP effects at ground level. Once the nuclear bomb's parameters are defined, predicting nuclear HEMP environments with computer-based models is a well-established capability in the United States.

The hostile nuclear EMP environment is created by the gamma-ray output (as well as x-rays and bomb debris for exo-atmospheric bursts) from the nuclear explosion (the "source") and the subsequent electron generation and dynamics within the atmosphere and magnetic field perturbations outside the atmosphere. Nuclear bomb explosions at high altitude in the atmosphere and in near-Earth space create three distinct components of EMP threats that are characterized by the timeframe over which they occur after the burst (from nanoseconds to a microsecond, from microseconds to a second, and from a second to many minutes). These electromagnetic threats are termed the E1, E2, and E3 components of nuclear HEMP. Each EMP threat component has different electric field strengths (typically ranging from kilovolts per meter for E1 to volts per kilometer for E3) and frequency content (ranging from many hundreds of megahertz to many hertz) that ultimately determine how

much current is "coupled" into which parts of the exposed power-grid infrastructure elements, and whether or not that component will be temporarily or permanently disabled.

The EMP waves travel downward (or "propagate") to the ground at the speed of light, exposing objects to the EMP threat waveforms. The amount of damage, if any, to the exposed electronics (for example, grid control centers and supervisory control and data acquisition, or SCADA, elements) and objects (such as transformers) connected to long electrical conductors (such as long power and copper communication lines) depends on how much energy in the form of induced electric current couples into the object or item that was exposed to the EMP. The added current going into an exposed electronic component or item of electrical equipment represents an "insult," over and above the normal operating conditions within the component that can then cause an upset or burnout of the object. The U.S. nuclear EMP effects community has the computational ability to model the created EMP threat waveforms from the source and propagate them down to the ground and thereby to exposed objects. This community is also generally able to calculate how much current is induced in exposed conductors (for example, long lines) and well-defined discrete objects (such as buildings and electronics boxes). However, the more complicated the exposed object's design and geometry (for example, the design and geometry of a transformer), the more difficult it is to computationally model the induced current. Therefore, experiments are also conducted to help characterize the induced, or coupled, current insults as a complement to computational modeling approaches.

The ultimate response of the exposed component or subsystem depends on the magnitude of the incoming current insult (how many amperes and over what timeframe). Sometimes, the high current insult burns out a sensitive device or circuit inside the exposed object, and the item is then permanently damaged. That is, the component will no longer work, and it would need to be replaced with a new component before system functionality and operability could be restored. For more moderate incoming current insults, local heating is generated inside the object because of current dissipation, and the local heating can have a temporary disruptive effect. Once the generated heat inside the object is dissipated, the object can return to normal functionality, but sometimes this return to functionality occurs only after human intervention to power down and power up the object. If the incoming current insult is low and not significant, the object can absorb the current insult and continue operating as designed. If the component is simple (for example, an electrical circuit or device), we can model the response of the exposed object to the current insult and thus determine whether it would be upset or damaged. However, many electrical components, subsystems, and even integrated systems have complex designs and constructions, and therefore we must resort to a combination of computer-based models and experimental test-based approaches to understand their response to the EMP-caused current insults. For complex, interdependent linked systems, such as the U.S. power grid, it is essential that computational and experimental modeling approaches be combined in order to verify and validate that the correct problem is being modeled and acquire the right level of confidence in the results.

Once an electronics-based device, component, subsystem, or system has been fully characterized to nuclear HEMP threats and has been found to be susceptible or vulnerable to the EMP-induced current insult, adverse effects (such as temporary or permanent failure) can be mitigated in several ways. One would want to consider mitigating the adverse affects, especially if that component is a critical element in a larger networked system. A common approach for mitigation is to harden the exposed object(s) against the EMP threat using a range of well-established design hardening techniques, such as faraday-cage shielding, grounding, filters, fast-acting current shunt devices, and responsive control systems to manage the effects that could start to cascade across a larger network of linked objects. If hardening against EMP effects is done early in the design definition and development process, before manufacturing, it can be added in the easiest and most cost-effective manner. The designer must know ahead of time the expected nuclear HEMP threat environments and the required level of hardness for the exposed component or subsystem needed for continued operation after the EMP attack.

The U.S. electric power grid contains some level of inherent hardness to the three nuclear EMP components. E1 (the high-frequency component) corresponds to electromagnetic interference threats from nearby transmitters (for example, cell-phone, radar, TV, and Wi-Fi transmissions), and electromagnetic compatibility standards are followed to protect against such electromagnetic threats. The E2 (mid-frequency) component corresponds to the EMP from nearby lightning strikes, which the power grid is already protected against. Finally, E3 (the low-frequency component) corresponds to solar-induced geomagnetic storms and the resultant ground-induced cur-

rent threats, which the power grid is already resilient against to a degree and is more resilient against in some northern latitudes.

A key unanswered question remains: How much more severe would the full range of possible nuclear-driven E1, E2, and E3 components be, and what level of protection would the existing power grid have against HEMP effects generated by a nuclear detonation? The answer depends, in part, on the type, yield, and detonation altitude of the nuclear bomb that produces the HEMP effects, the real-world orientations of power grid elements relative to the detonation, any inherent shielding properties of the exposed infrastructure elements, and the robustness of the exposed elements to withstand the EMP insult. More computer-based modeling and simulation, as well as experimental testing, would provide a basis for a more complete understanding of the response of the power grid to a HEMP attack and of the specific hardening measures to be considered for addition to the grid.

As new technologies are studied, developed, and added to the power grid (such as smart grid monitoring and control), being aware of and considering the evolving threat space (for example, intentional electromagnetic interference) and natural environments (such as variations in solar geomagnetic storm intensity) that could affect the performance and reliability of the new technologies may offer opportunities to add some level of inherent hardness against specific nuclear HEMP environments.

Assessing the Risks Posed by Nuclear High-Altitude EMP (HEMP) Attacks

In assessing the risk posed by nuclear HEMP attacks, we use the classical risk equation, where risk is expressed in terms of likelihood (or probability) of the attack, susceptibility (or vulnerability) to the hostile environments created by the attack, and consequence (or system-level impact) as a result of the attack.

In Sandia team's view, the likelihood of a nuclear HEMP attack occurring above the United States is very remote. The advanced nuclear weapon states have had the capability to do significant damage against the United States and our power grid for many decades, but they have been and hopefully will continue to be deterred from such attacks by a strong U.S. strategic deterrent. Some argue that terrorists who might someday gain possession of a nuclear device can conduct a similar type of attack and generate the same amount of damage. According to the team, the assertion that terrorists can use a nuclear warhead in a crippling HEMP attack against the United States is not credible, and the likelihood of something like that happening is low. More detailed explanation can be provided in a classified venue.

In terms of actual susceptibility of the power grid to nuclear HEMP effects, the limited available data on damage effects make it difficult to know what will precisely happen to exposed elements across the grid, especially to the large high-voltage transformers. Given the amount of investment associated with potentially hardening against EMP effects, additional computational analysis and testing are needed for higher confidence in whether and to what extent exposed elements are susceptible to any temporary or permanent EMP damage effects. While computer modeling work to date has been extensive on the induced currents on exposed power lines, very few experimental data exist on how the exposed grid elements (the controllers, protective devices, high-voltage transformers, etc.) would actually respond to higher than normal currents. Highly instrumented testing of key power-grid components to E1 and E3 threat insults is recommended and should include characterizing how failures (physical damage) occur and at which insult levels they occur. Such data would help validate existing power-grid models, reduce inherent uncertainties about the amount of damage induced, and provide more confidence in the results.

Finally, not enough data exist to confidently assess the extent of any power-grid outages from a nuclear HEMP attack and the amount of time needed for recovery. Several real-world examples have been studied of how the grid might respond to E3-like effects (for example, the March 1989 Hydro-Quebec grid collapse due to a severe solar geomagnetic storm and the August 2003 power outage in the Northeastern United States), and table-top exercises have been developed on how utilities would find and fix the resultant EMP-induced damage and bring the grid back online after a certain period. However, one can only parametrically evaluate the impact of nuclear E1 and E3 attacks because we do not know the level and extent of damage that would actually occur. If additional data were to become available on E1 and E3 damage effects and lethality levels of critical power-grid components, then the basis would exist for more-confident U.S. power grid simulations of the extent and magnitude of damage and the resultant recovery times.

SUMMARY AND CONCLUSIONS

From an integrated "total" risk perspective, the Sandia team considers nuclear HEMP threats to be of remote likelihood. Also, the true extent of the grid's suscepti-

bility and vulnerability to such effects (be they temporary, permanent, or even not present) and the resulting consequences (damage extent and period they would be lasting) are mostly unknown, except for the assumed worst-case environments and assumptions made in the current nuclear HEMP threat studies that the Sandia technical peer review team evaluated. We commend FERC and the authors of the studies for their excellent work to date on evaluating the impact of EMP threats to the U.S. power grid. However, we respectfully suggest that more computational and experimental work is required before fully informed decisions can be made about where and to what extent the power grid should be hardened solely against nuclear HEMP threats. If the decision is made to protect the power grid against a broader set of likely EMP threats, including solar geomagnetic and electromagnetic interference threats, then an awareness of nuclear HEMP environments and effects should also be considered.

The Sandia technical review team recommends that this complex problem be studied in more depth in order to include results from additional computer-based simulations and experimental testing. Specifically, under nuclear HEMP threat conditions, how do high-voltage transformers and their protection and control elements respond to the range of induced current insults, and if they fail, how do they fail? Answering such questions would provide critical data to enable better understanding and validation of results by advancing a complete understanding of all the risk elements, as well as quantification and reduction of uncertainties in order to fully inform decisions that may be made about the U.S. power grid. We suggest that a graded hardening approach could be considered, whereby selective hardening could be accomplished easily and cost-effectively, in combination with addressing new and emerging threats to the grid (for example, intentional electromagnetic interference). Also, by further evaluating the consequence of EMP attacks on mission-critical U.S. installations and functions (for example, important U.S. war fighting or continuity of operations), specific sites may be identified that may require selective EMP hardening.

The CHAIRMAN. Thank you all very much. Let me start with a few questions here.

Mr. McClelland, your testimony, as I understand it is, that the Commission's legal authority is inadequate and that the draft legislation that we've prepared address many of those issues. Can you be more specific as to the ones we are not adequately addressing?

Mr. MCCLELLAND. The draft legislation provided the Commission with the ability to address vulnerabilities rather than wait until there was a designation that there was an imminent danger. The legislation allows the Commission to address the vulnerabilities. We believe from the read that it also addressed a situation where it may not be appropriate or it may not be possible to wait for the ERO to develop a standard to address a specific issue.

For instance a particular threat against a utility or a grouping of utilities that serves a particular military base. There may need to be some interim action that they take. It wouldn't necessarily be applicable to other utilities.

We believe from the read that we have that the Commission wouldn't have to wait until the ERO made a designation about a particular standard or attempted to craft a particular standard to address that circumstance. The Commission would be able to move directly to address that issue.

The CHAIRMAN. You're giving us an example here.

Mr. MCCLELLAND. Yes.

The CHAIRMAN. Where the draft does give you, in your view, the authority that you would need to deal with a situation. Are there instances where you think the draft fails to give you the authority you need to deal with particular situations?

Mr. MCCLELLAND. No, not in particular. There are areas where the Commission does not have authority under 215. Some of those

exclusions, for instance, for allowing Alaska and Hawaii continue. But the draft does address that circumstance in another manner.

Except, I guess, the point would be that if it addresses—if it allowed the Commission to address vulnerabilities. If it allows the Commission to reach beyond the definition of bulk power system. If it allows the Commission to address EMP and non cyber aspects, then it would address the issues that I raised in the testimony.

The CHAIRMAN. OK.

Ms. Hoffman, did you have any comment on any of this?

Ms. HOFFMAN. No, I don't have any comment.

The CHAIRMAN. OK. Let me ask on this EMP thing because I heard your testimony, Mr. McClelland. You were talking about EMP generally, as I understood it.

You had this particular reference in here which I thought was pretty startling where you say that the study has been done assessing the 1921 solar storm which has been termed a one in 100 year event. Applying that, what happened in that 1921 solar storm to today's power grid. The study concluded such a storm could damage or destroy up to 300 bulk power system transformers interrupting service to 130 million people for a period of years.

That's very different than what Mr. Tedeschi was referring to. As I understand it he's talking about the electromagnetic pulse problem which could be created by a nuclear blast intentionally by someone. I guess I'm just unclear.

You think you don't have the authority to take the appropriate or to require the appropriate hardening to deal with either of those circumstances? Is that what I understand?

Mr. MCCLELLAND. The Commission's authority is coupled through the Standards Development Process. The Standards Development Process is too slow. It's too unpredictable. It's too open to address national security threats.

So the Commission may order a standard be returned on a particular matter. But it can't be prescriptive or specific. It can't write the terms of the standard. It can only turn the standard over to the ERO for standards development.

The CHAIRMAN. OK. So I think, I believe Mr. Owens made the point that there are 2, sort of, parts of this problem we're trying to deal with.

One is the problem of potential vulnerabilities. hat would be the electromagnetic pulse issue.

Then there's the other part of it which is the potential of imminent threats and the ability of the Commission to act or the ability of anyone to act quickly to deal with immediate imminent threats.

You're basically saying that you believe something like what we've got in draft form here is essential to shore up the ability of the government to deal with both sets of problems?

Mr. McClelland: Yes. It would allow the Commission to address a sophisticated and targeted attack or an event aside from the Standards Development Process. That's right.

The CHAIRMAN. OK.

Senator Murkowski.

Senator MURKOWSKI. Thank you, Mr. Chairman.

Just to follow on to the questions here. I direct this to you, Mr. Tedeschi. When we're talking about the EMP attack or geo-

magnetic disturbances, these are not new in the sense that we're just now learning of them.

So given the knowledge, given what we have in terms of the potential for these types of disruptions. What have we done to date in order to protect the grid? I'll ask you and then if others can step up here.

Mr. TEDESCHI. Senator, I would just suggest that the geomagnetic threats mimic part of the nuclear EMP threat space. The geomagnetic threats do occur with regularity. The severity of those is ongoing in terms of our scientific understanding. Those threats have manifested in the past.

There are examples where elements of the grid have gone down. The utility owners, NERC, FERC, others, have responded to those. In some cases, added some of a hardening against the geomagnetic EMP threats.

Our view on the nuclear electromagnetic threats there's the component that mimics the geomagnetic threats that it's a very low likelihood of occurrence. So from our perspective if the utilities, if NERC, FERC, the legislation, allow DOE and others to harden against the geomagnetic threats, which are real and do occur. That that will provide an inherent level of hardness against nuclear EMP threats if those were to occur someday.

But I think others are more able to answer the question of likelihood and the severity.

Senator MURKOWSKI [presiding]. Ms. Hoffman.

Ms. HOFFMAN. Part of the problem is a natural progression over time. Some of the older transformers may have some weaknesses in them that make them more vulnerable to any sort of event. Some of the newer transformers in use have a stronger capability to withstand certain incidents.

Part of the discussion and the investigation that needs to take place is what level of protection do we want to require transformers and the electric grid to have, what level of event should they be able to withstand? Do we want to protect against the 1921 event with very high induced currents or do we want to actually look and say here is a median level of event which the industry should progress to protect against with respect to transformers, with respect to harmonics on the electric system. So a lot of this discussion comes down to the parameters that we should be building the technology to withstand.

That's the direction I think the conversation is evolving toward.

Senator MURKOWSKI. Mr. McClelland, did you want to go ahead?

Mr. MCCLELLAND. Sure. There are operational procedures in place today where if the industry is alerted then they can take precautions to go in the more conservative operations to protect equipment. The problem is though that we haven't seen a 1921 event.

A 1921 event, we found from our assessment, could be catastrophic in nature to the grid itself. So the question would be not so much as to what level we dampen to, but can we block all events. The answer we think is, yes.

But there's still some work to do as Mr. Tedeschi pointed out. We still need to identify the proper equipment. Test the equipment. Then move for mitigation against these events.

Then we wouldn't have to worry about whether we have a 25 year event, a 50 year event, a 100 year event. If we block it, it's taken care of. It's an automatic mitigation method. We don't have to rely so much on human intervention to save the grid in a circumstance like that.

Senator MURKOWSKI. Thank you.

Mr. MCCLELLAND. But to also answer your question directly. There's been very little, if any, hardware mitigation that's been put on to protect from say, solar magnetic disturbances on the grid.

Senator MURKOWSKI. Thank you.

Mr. Cauley, you want to finish it up?

Mr. CAULEY. Thank you. I really think that Mr. Tedeschi's testimony hits on the issue of sorting out the key issues. We're focused at NERC and I think working with the industry to resolve the solar magnetic, geomagnetic issue.

We did have a major storm in 1989 that blacked out Quebec. I think the industry learned from that. There was a lot of equipment hardening in the northern latitudes where it's more of an impact.

I think as we look at the risks of a larger storm we have to ask ourselves, you know, how much further down into the continent would it extend. So we are working to upgrade notice procedures, advance warning systems and also doing engineering studies. If we did the hardening, as being suggested here, it will affect other issues like clearing of electrical faults and the dynamic behavior of the system.

So we have to study it. Be very careful about changing the system in a way that does not cause harm in other ways. So we're focused now on this solar magnetic and geomagnetic disturbance issue right now.

Senator MURKOWSKI. Thank you. My time is up.

I just want to ask very quickly. Is there a greater incidence of the solar magnetic, electromagnetic in the northern altitudes?

Mr. CAULEY. Yes. The impact, depending on the—it's a very dynamic situation. But if the pulse hits the Earth's magnetic field that the disturbances most severely affected in the northern latitudes. So the larger the pulse from the sun, the further down it can extend into the middle latitudes of the United States.

Mr. MCCLELLAND. May I just quickly add to that? Our study did consider the likelihood of a solar magnetic disturbance over Winnipeg, Manitoba verses Minneapolis, Minnesota found that they were equally likely to occur. In fact if it happens over Minneapolis, Minnesota the number of bulk power system transformers that could be damaged/destroyed reaches over 1,000 rather than 368 which was on the Winnipeg, Manitoba incidents.

So it can center. But it can also—it can move around. We just don't know where it will be. We don't know when it's going to happen again. We just know with certainty that it will happen again. It's inevitable.

Mr. OWENS. May I add to this conversation just very briefly?

I do agree in what they're demonstrating is there's no perfect solution. Mr. McClelland made a reference to the potential destruction of 300 transformers as he related back to the prior major solar activity that we had in 1921. One of the things that we're seeking

to do in the industry, we're working very closely with NERC is to harden our systems, create redundancy in our systems.

With respect to transformers, we are making sure we have spare transformers. We have a very substantial spare transformer inventory that the industry, for several years, has been committing resources to because we recognize how critical the transformers are. If you lose a transformer it takes a while to restore service.

So we're working to make sure we have this redundancy in our transformers. There are other elements, critical elements of our network as well that we're looking at. But there's no perfect solution.

It's very important that you have the redundancies and the hardening of the system. But it's equally important that you're able to restore service as quickly as possible.

Senator MURKOWSKI. Thank you all. I am way over time. I apologize to my——

The CHAIRMAN [presiding]. No problem.

Senator Burr.

Senator BURR. Thank you, Mr. Chairman. As interesting as EMPs and solar magnetic pulse is, I'm going to try to stay away from that.

As the only member here today of the Intelligence Committee, I'm going to try to focus on the realities of the threat that's out there and maybe the options that we have. Ms. Hoffman, what analytical assets does the DOE have to identify any intelligence threats?

Ms. HOFFMAN. The intelligence cyber threats comes through the Department, Office of Intelligence shop, not through our organization, the Office of Electricity. We coordinate with our intelligence office as well as with DHS.

Senator BURR. The analytical work for what the DOE receives is from multiple sources.

Ms. HOFFMAN. Yes.

Senator BURR. It comes from DOD. It comes from DHS. It comes from NSA which is part of our problem.

Now Mr. Cauley, if I understood your testimony correct, NERC currently has direct contact with the intelligence community. Is that correct?

Mr. CAULEY. That's correct, Senator Burr, with multiple agencies.

Senator BURR. So you're part of that intelligence loop right from the analyst?

Mr. CAULEY. Those are primary sources that we use to get information to industry to take actions. We have, myself, top secret clearance and others on staff have clearances to receive that information.

Senator BURR. OK.

Mr. McClelland, where does FERC currently get their intelligence from?

Mr. MCCLELLAND. We get our intelligence from DOE, CIA, NSA and DHS.

Senator BURR. OK. How many people have the security clearance to say, sit down with CIA to get information from them?

Mr. MCCLELLAND. We have 3 people in our organization that have SCI clearance. I couldn't give you the specific number, but we have several more that have TS clearance. All of our chairman and all commissioners have TS clearance.

Senator BURR. Under the joint draft, FERC would be authorized to develop standards to address cyber security vulnerabilities for utility generation, transmission and distribution. Who currently has jurisdiction over the distribution system?

Mr. MCCLELLAND. The States do.

Senator BURR. Under this would that then supercede the existing authority?

Mr. MCCLELLAND. I think the way the legislation is written, I think the Commission would have the ability to write cyber security or non cyber standards for distribution.

Senator BURR. Let me ask an open question. Why should we give FERC, who is the economic regulator of markets, jurisdiction over distribution?

Mr. MCCLELLAND. Section 215 of the Federal Power Act gave FERC jurisdiction over both cyber security and reliability standards.

Senator BURR. I realize we did. Understand that today. We were very early into sort of the threat——

Mr. MCCLELLAND. Right.

Senator BURR. Generation that we're in now. Personally if I had it to do over again, I'd love to see the focus of this on how we remove the authority that we gave to FERC. Because I believe as a country right now, we're—we've got the authority in too many different places to be responsible for a threat stream that by the time these agencies are notified, quite frankly, it may be too late for the immediacy of a threat. I was more impressed with Mr. Owens' answer, even though it was on EMP and solar magnetic.

The industry is making the advances that they need to to respond, to get back up and running. The NERC, if we need to look somewhere, I guess our question should be what additional authority to you need to do what you're currently doing verses to bring anybody else new into the process of mapping out a pathway forward for the infrastructure and its integrity?

Mr. Cauley, I'm giving you an opportunity. What do you think?

Mr. CAULEY. If that's a question, Senator Burr. I did point out in my testimony that the one gap that I sense right now is if there is an imminent threat or vulnerability and we need industry to take action then we do not have the ability to make enforceable directives to industry. That has to be done very carefully.

I'm not an operator. Mr. McClelland is not an operator. We don't want to order the industry to take an action that has risky consequences.

Senator BURR. If you were to take an action or if we were to give you the authority over distribution and you made determinations under the guidance of cyber vulnerability. Who pays for it? Who pays for that?

Mr. CAULEY. The rate payers.

Senator BURR. Rate payers. Let me just suggest to you regardless of how we move forward. Let's consider the fact that the rate pay-

ers are going to pay for this. We don't have the luxury of doing everything that one might think we should do to protect ourselves.

I would only say this as a member of the committee, you can't do enough things to protect us 100 percent from the threats that are out there. So let's recognize the fact that there's got to be some consideration on cost and a big consideration on who pays for it.

Mr. McClelland.

Mr. MCCLELLAND. I wanted to say one other thing to revisit the point that you had before about distribution. The problem with distribution is that if there are 2 way communications between distribution and say, the bulk power system. You know from your experience that any time there's 2 way communication there's a chance for corruption. Currently there are 50, say 50, different agencies maybe looking at cyber security, maybe not.

We've got wide scale deployment of smart grid equipment that depends on 2 way communication. So all I'll say is regardless of where that authority falls there is a gap in the authority. Is a significant gap that comes to cyber security. Thanks for——

Senator BURR. I appreciate that comment. This would be a personal observation with what we don't know today. I'm more encouraged to slow down the implementation of smart grid technology until we learn the things that we need to learn to implement it with a great deal of confidence.

Thank you.

The CHAIRMAN. Senator Udall just arrived, but he has indicated that he would like Senator Lee to go ahead with his questions before he does questioning. So go ahead.

Senator LEE. Thank you, Mr. Chairman. Thanks to all of you for joining us here.

The joint staff draft would give authority to DOE and FERC or a combination of the 2 of them to order electric utilities and others to take action to overt imminent danger that could stem from an imminent cyber security threat. If what we're talking about is cyber terrorism does it make sense to put that authority in any of the agencies that deal with intelligence? For example, the intelligence agencies that are gathering the information that would signal this sort of a threat or does it make more sense to put it in a Federal regulatory agency that deals specifically with energy?

Ms. HOFFMAN. To begin with, the approach has to be comprehensive. It has to involve both FERC and DOE, in fact the whole government. The intelligence agencies do a very good job in analyzing the information. The operators are the folks that actually look at the operations of the systems will be best to help develop the mitigations and the solutions.

From my perspective it's a partnership that's required.

Senator LEE. Is this, following up on Senator Burr's line of questions. Is this something that necessarily needs to be Federal? Is this something that could not be done on a State by State basis with State regulators working in concert with Federal authorities? In other words from a regulatory standpoint should the regulator be Federal or should the regulator be State?

Mr. OWENS. I might seek to respond to that, Senator.

I think you have to make a distinction between an imminent threat and a cyber vulnerable assets. With respect to an imminent

threat it makes sense to me to believe that you need a Federal agency that sees that intelligent information. So you can act decisively.

I spoke earlier about the need for horizontal communication. So it means that the FERC, as an example, and the Department of Energy and the Department of Homeland Security, all those agencies, those who have intelligence about the imminent threat and those who have the understanding and the authority to order a change in operations. They should be working collaboratively.

When you look at the issue of a cyber vulnerability, a critical asset, that takes more time because what you want to do is you want to make sure that you've hardened the system and you've prevented a potential cyber disaster in the future. That requires coordination with the industry. It requires complete coordination with the government agencies are affected.

Where it gets real controversial or difficult is if you suggest that all assets need to be looked at by one Federal agency. When we recognize that we also have State bodies that look at these issues. It seems to me a very clear way to do this is to make sure that there's that vertical dialog between the Federal Government and the State agencies, who daily deal with these issues as well.

They deal with cyber threats at the distribution level. They work very closely with their local law enforcement agencies. They work closely with the FBI. They're very much aware of some of these threats that are involving their local utilities.

What I believe is important to make sure is we don't have a gap. I don't believe we have a gap. I think those agencies are taking on their responsibilities very forcefully. I believe those agencies, those State agencies are working very closely with the Federal Government in trying to understand what those imminent threats are and the actions that have to be taken.

So I would encourage us not to give the impression that the State agencies aren't doing their job because they are.

Senator LEE. Mr. McClelland, I wanted to follow up on a different issue with you. You referred to the fact that if we had another 1921 style event that it could knock out, did you say 300 transformers?

Mr. MCCLELLAND. Over 300. It could affect over 300 transformers, 368 is the exact number.

Senator LEE. Potentially affecting how many customers?

Mr. MCCLELLAND. 130 million customers.

Senator LEE. I think I heard you say that some of those could be affected over a 10-year period is——

Mr. MCCLELLAND. No. Yes, they could be affected. There could be service interruptions for over a 10-year period.

Senator LEE. That's simply because it could take that long in order to restore all the equipment that would be destroyed by the one event.

Mr. MCCLELLAND. Right. The bulk power system transformers are typically about a 52-week or 1-year lead time. They're not produced in the United States anymore. We are dependent on other Nations to bring them forward.

There is an existing queue of transformers that need to be built. Developing Nations such as China are using lots of those slots in the queue, the ordering queue for those transformers.

Senator LEE. OK. Is there anything we could do in that circumstance to shorten that time period? I mean, I assume we could ramp up production of those.

Mr. MCCLELLAND. Yes.

Senator LEE. Faster, so you're presupposing that were—that our production rate would be roughly what it is now.

Mr. MCCLELLAND. Right. We could attempt to attract manufacturers to the United States. We could ask for expedited delivery. Perhaps pay some fee to have expedited recovery. But there's not a lot more than that.

The transformer capacity is the capacity. So other people would have to get out of the queue, stand aside, for us to have those units built. Even then the through put of those facilities is limited.

Senator LEE. OK. I assume it's not pragmatically plausible. I'd say it's not possible or practicable to produce a transformer that is immune from this sort of pulse.

Mr. MCCLELLAND. There are blocking devices that can be employed. The devices are not widespread though. They haven't been deployed.

So there are conceptual ideas that we've seen. They need to be prototyped and tested. I'm an electrical engineer having spent almost 27 years in the business. My recommendation would be to automatically block this on the most susceptible or most critical elements of the bulk power system so we don't need to stand in line after a solar magnetic disturbance to wait for transformers.

Senator LEE. OK.

Mr. MCCLELLAND. One thing, if I could just revisit very quickly. FERC is more than an economic regulator. My office has about 135 employees. Most of those employees are electrical engineers with advanced degrees with vast experience in the electric utility industry.

Senator LEE. OK.

Mr. MCCLELLAND. So we do have expertise with——

Senator LEE. Just going to the technological expertise within your agency that could qualify you to——

Mr. MCCLELLAND. To deal with——

Senator LEE. Deal with these situations.

Mr. MCCLELLAND. To deal with new section 215. That's not to minimize what DOE or what the industry does. But it is to fairly represent what we do at our agency.

Senator LEE. Thank you. That's all.

Mr.MCCLELLAND. Thank you.

Senator LEE. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Udall next and then Senator Hoeven.

Senator UDALL. Thank you, Mr. Chairman. Good morning to all of you.

This is an important and timely hearing, and I want to acknowledge the leadership of the ranking member and the chairman. I sit on the Armed Services committee. I sit on the Intelligence Committee. I sit on this committee.

This is a truly complicated challenge for us. There are many entities and agencies involved. But all of that doesn't lessen the threat. I think the longer we delay obviously the more we may experience an incident that we will regret.

The military is moving aggressively toward islanding some of their facilities. Because I think they see that as a necessity. So my appeal to all of you and all of us is to focus on this and truly get something done in the near, near future. In that spirit, hope there's a bit of positive thrust in that spirit.

But I want to turn to the Secretary and Ms. Hoffman. In the report just last month, April 2011, MacAfee and the Center for Strategic International Studies, CSIS, stated that the "adoption of security measures continues to grow," but "unlike threats and vulnerabilities, adoption of new security measures is improving at a snail's pace." Do you think that characterization fairly describes our Nation's electric industry?

Ms. HOFFMAN. The adoption of technologies is slow.

First of all we have to look at the availability of new technologies to address security issues. The cyber security environment is changing on a real time basis. The capabilities of the adversary are also changing. But it takes time to deploy new technologies, and the electric industry tends to follow a longer timeline with respect to transferring out older technologies and bringing new technologies in.

So there are several factors compounding an already complex issue. What we need to do is enable technologies to be upgraded in a more timely fashion. We also need to continue to test new technologies. We also need to build a stronger work force so that as we move forward we can get better adoption of the technologies into the system.

Senator UDALL. Do we need to call—I know we do this in this town, but a summit of all the stakeholders and look at that Gordian knot sitting in front of us and all maybe, put our hands on the sword and cut through it? My concern is that we continue to point fingers in every single direction. Nothing is really going to happen until we're forced to react.

That's not the right position to be in.

Ms. HOFFMAN. We need to continue to have dialogs to get ahead of the game. It comes down to understanding what are the priorities for the issues we need to address, analyzing are we actually complete in our strategies, and whether there are any gaps with respect to protecting the system.

Then we need to make sure that there's a comprehensive look at what the impact and the costs are of implementing new strategies and solutions.

Senator UDALL. Mr. McClelland, if I might turn to you. Could there be circumstances where FERC ought to have the capacity to just order measures first rather than work through the ERO?

Mr. MCCLELLAND. Yes. I think there could be. I really think that those circumstances should be very limited and should be emergency type circumstances.

There may be a particular instance where CIA or DOE or DHS uncovers an attack vector of vulnerability that could be exploited. Something like Aurora, maybe there's not enough information to

show that it's an imminent danger. But it's certainly a viable vulnerability. The facility that would be interrupted would be critical.

It may not be applicable then to everyone else. But that entity may need to go to a heightened state of readiness. They may be what we would term in case of emergency break glass scenario where they disconnect remote operations at some facility for some period of time.

There could be limited circumstances like that where a standard wouldn't be appropriate. But it would be very important to FERC to move quickly if it's given this authority, to order those mitigation measures to work with the affected entity to get those in place.

Senator UDALL. I want to give Mr. Cauley a chance to comment.

But I would add this observation. I serve in the U.S. Senate. We have 50 States represented here. We can be very decentralized. We can be very focused on our own regional or State interests. So I have some sympathy for the challenges that you face. But I appreciate your comments in this regard too.

Mr. CAULEY. I think there is a need, Senator, for some, as Mr. McClelland is suggesting, some ability to get information and actions out to industry quickly. But I don't know of any one place or any one authority who is the smartest on the planet, who knows the right answers all the time. Can issue that order without any risk. So I would encourage whatever we end up with that there be the opportunity for consultation with those who have to be involved in that decision.

I think the perception that's been painted that the industry really hasn't done anything and is slow is a false one. I'd encourage any of you in your own States to go visit your local utility control center who fall under our standards.

You will have a hard time getting in. You certainly won't touch any of their computers. They'll ask you for devices that you have on you. It's like going into a government facility.

So I don't think the industry likes to advertise how secure they—all the work they've done to secure our systems. But there is a lot of work going on.

In our standards we've found—this number may be corrected, but at least 1,500 violations of cyber security standards. So we are actively out there beating on this day in and day out. Folks are fixing it. So it's not like we're standing still.

Senator UDALL. Thank you.

The CHAIRMAN. Senator Hoeven.

Senator HOEVEN. Thank you, Mr. Chairman.

I'd like to follow up on Mr. Cauley's statement. Ask each of you just—and I'm trying to get a sense of consistency or where there's differences in your opinion. How secure is our system? Is it secure? Is it very secure? Is it secure or do you think it needs significant improvement?

I am looking for kind of like say, following on your statements saying that boy there's a lot of work being done. Generally I get the sense you feel the system is secure. What is everybody's opinion in that regard?

Ms. HOFFMAN. I will first say it depends on what we're securing against—from known issues where we can share the information with the industry or unknown issues.

Senator HOEVEN. Let's just start with a cyber attack of some kind. Somebody trying to put in a worm or some type of, you know, software attack of some kind to disrupt the system.

Ms. HOFFMAN. There is a level of security out there already. Yes.

Senator HOEVEN. That's pretty, kind of, noncommittal, so.

Ms. HOFFMAN. OK.

Senator HOEVEN. So we're secure or?

Ms. HOFFMAN. We're secure to a point. There are vulnerabilities with human interface, so that if it's a worm or some human interaction continues to perpetuate that.

Senator HOEVEN. Recently the Israelis developed a cyber attack on the Iranian nuclear power development system. Could that type of worm be put into our system and disrupt power supply in the United States?

Ms. HOFFMAN. I don't have the specific details on those worms. So I can't give a very good analogy to that specific example. The issue is there's always room for improvement.

What we need to do is to react quickly, be very quick on our feet, be able to deal with any sort of event that comes out. The industry needs to react quickly to the event. One of the things we need to do is to provide for information exchange so that we can act quickly. That is the capability we need to go after.

Senator HOEVEN. If the Secretary of Energy has the ability to intervene in that type of event or concern that that type of event occurs. How is that decision made? How do they intervene?

Ms. HOFFMAN. With respect to the Secretary of Energy, under the Cyber Space Policy Review, there is a national incident management process under development in the Federal Government. DHS has a national cyber security control center that we all participatein within the energy sector. ISAC also participates in that.

When a cyber event occurs, the information is shared. Next a coordination group is formed that identifies the potential impacts and consequences and the potential mitigation solutions.

Senator HOEVEN. So then if each of you would just comment in terms of what you perceive that risk to be whether it's a high risk or whether we have strong security in place that would mitigate it and our ability to react.

Mr. MCCLELLAND. Really when you're talking about as many utilities as you are, you're talking about absolute worst practices up to absolute best practices. So it depends on the entity that's defending and it depends on the entity that's attacking.

But with that said, if my personal level of confidence is not high. Because if the government agencies can't protect against a sophisticated Nation, State threat, advanced persistent threats that we've seen. I don't think that individual utilities will be able to.

As tightly interconnected as the utility system is, it doesn't take much. It doesn't take many penetrations or many disruptions of pieces of equipment to cause profound analogies within the interconnections themselves.

Senator HOEVEN. Our ability to react in the event of that type of an attack?

Mr. MCCLELLAND. Again, it depends on the piece of equipment that's attacked. If it's a large generator, critical size generator and

if it's a simultaneous attack on several of those facilities, those generators can take years to construct and put into service. So prolonged outages or prolonged disruptions or prolonged cases of reduced output, could be possible.

Mr. CAULEY. Senator, the challenge you're hearing in the responses, I think the answer is both. I think systems are secure at a baseline level. I think there's the training. There's the tools, the procedures.

The challenge is there are threats that exceed the normal capability and awareness of a civilian infrastructure. That's where the interplay between the Federal Government, who has intelligence of emerging threats and actors who would do things coordinated wide area attack on physical facilities, a very wide coordinated cyber attack that we're not aware of. But the practices, the normal prudent practices, I would say the industry has a handle on those. Those are things they're aware of.

It's the emerging things from threats that we don't have sufficient tools at this point that we would like to make sure there's a good coordination between government and industry. What is it we're seeing? How can we be respond and react to those kinds of things?

Mr. OWENS. I think he said it well. It requires, as I was stressing earlier, tremendous coordination involving the government and industry. We've hardened our systems. But as was said earlier, there's no perfect system.

We have to be able to restore service quickly if there's an outage. We have isolated assets that we think are very critical that provide some cyber vulnerability working very closely with NERC and with the Federal Energy Regulatory Commission. It was mentioned earlier about the new technology called modernizing the grid or the smart grid.

We're making sure that the equipment that we're installing to make that grid much smarter, that they're high cyber standards that have to be met by the vendors and the manufacturers. So it's an evolutionary process. It's not a static process.

Our systems are not perfect. We are building redundancies. But again, there's still a lot of work that needs to be done. But it requires complete coordination between industry and government.

Senator HOEVEN. Sir?

Mr. TEDESCHI. Senator, I am not a cyber expert. So I must defer on answering the question.

Senator HOEVEN. Alright. Thank you.

The CHAIRMAN. Let me ask about one other issue that's come up in the testimony that some of you've presented here. That is the whole issue of authority over the distribution systems. As I understand it we've got FERC's authority is under the Power Act is over the bulk power system. We're trying to also deal with this cyber security threat in terms of the distribution systems because the whole thing is integrated.

Let me just ask you, begin with you, Mr. McClelland, as to what your thought is as to what has been proposed in our draft to extend the authority to the distribution systems and what should be proposed and whether what we've got here is the right solution or whether there should be a different solution.

Mr. MCCLELLAND. I can comment on what's been proposed. Then I can also comment on what might happen if there's no distribution system protection.

What's been proposed, as I read it, is an emergency authority to address a vulnerability that would have a profound impact on the critical infrastructure of the United States, a strong impact. That authority would have to be used very judiciously, very infrequently. So it would not be a normal authority, but it would be an authority where say a smart grid installation is proceeding and millions of meters have the ability to provide a denial of service to some critical bulk power system facility.

At least in my personal opinion, that may trigger that authority to be used. Without an authority over distribution though, it would be up to 50 States to determine their policies as to how the cyber security might or might not work. It may not be consistent. It may mean that distribution systems would have to be treated as a non trusted source.

So from a verification, from a communication standpoint with cyber security, it would be placed in an outside realm. It would also mean that there would be no protection afforded to them by any sort of a Federal program, a Federal standards or a Federal jurisdictional program.

The CHAIRMAN. OK. Mr. Cauley, I think you have testimony in here about concerns that we would be in this draft extending jurisdiction, the FERC jurisdiction, to the distribution systems while your organization would not be able to extend any of your activities in that area. Am I understanding that right?

Mr. CAULEY. Yes, Mr. Chairman. Without taking a particular position about whether distribution should be included in the legislation or not, there are some concerns.

First off, I think our standards and the programs that we have in place work well to achieve the reliability and security of the bulk power system. The question is do we want to extend now that same protection to the distribution system I think was a policy question that I won't weigh in on. But if it were the case where FERC had authority that was beyond that of NERC I think it would be at all times we could be looked at as being deficient because our standards don't extend out to the distribution area.

So the point I made in the written testimony was I think to the extent we're going to cover cyber security between NERC and FERC I think the jurisdiction should be consistent between us.

The CHAIRMAN. But you don't think this distinction that Mr. McClelland is making between authority over to put in place standards to guard against potential vulnerabilities, that's one set of authorities.

A separate set of authorities is to take immediate action to deal with an imminent threat. You don't think it's appropriate that FERC have authority in that second area without NERC also having authority in that second area?

Mr. CAULEY. I think it's beneficial to have alignment with our—between the FERC and the NERC. As our process—essentially when we send out alerts or actions it goes out to the same companies. It goes out to individual companies that operate both transmission and generation and distribution.

So I think we would make the situation more complex and more difficult if we had, sort of, fractured jurisdiction.

The CHAIRMAN. OK.

Mr. OWENS. May I respond to that too, Senator?

The CHAIRMAN. Sure. Go right ahead.

Mr. OWENS. I would again go back to a distinction. For an imminent threat that puts our national security at risk, that puts our economic security at risk, I think it's very appropriate that the government act decisively and deliberately. That means Federal Government in close coordination amongst the various agencies that have intelligence information as well as the industry.

So I think that's a no brainer that we've got to act decisively to protect our society and our way of life and prevent disruptions. When we're looking at the issue of vulnerability, of potential vulnerability, of an asset that could lead to a cyber disruption that could affect our society, I think it's grey. That area gets very grey.

Where it gets grey is we know that the States already are dealing with that issue. I think that's what Mr. Cauley spoke to. I would have great difficulty if we said let's give FERC that authority and let them have that authority permanently to begin to develop standards that impact the distribution level, recognizing that we already have States that are intimately involved in these activities.

A standard implies that you have to make changes in investments, in your resources and so forth. There's a cost associated with that. Those State commissions have a responsibility of looking at those costs and the impact on consumers.

So I'd have great difficulty suggesting that we give FERC permanent authority over distribution assets when we already recognize the States have a vital role in this area. I think it would add tremendous confusion.

The CHAIRMAN. But I don't think that's what we're doing. As I understand what the draft does and what I thought I understood Mr. McClelland to say was that we would be giving FERC authority to take action to deal with imminent threats in the distribution system.

Mr. OWENS. I have no difficulty with that.

The CHAIRMAN. OK. So that's the limited authority. We're not saying from now on FERC has authority to set standards in the distribution system.

Mr. OWENS. OK.

The CHAIRMAN. I don't believe. Is that a correct understanding?

Mr. MCCLELLAND. I think there is a distinction here that's important to point out. So and I wouldn't argue with Mr. Owens' point. But there are 2 authorities.

One is for an imminent danger that goes to the DOE.

One is to address a vulnerability that could provide, you know, an impact, a negative impact on a critical infrastructure.

The difficult piece of this is to try define imminent danger. In a cyber security realm—I mean it's not as difficult if someone is setting up an intercontinental ballistic missile. You can look by satellites to see the launch pad.

For cyber security it may be a non descript building with 100 people attempting to probe the system. So as long at the threshold

isn't so high, imminent danger can be a very high threshold to prove. It may in fact mean that an attack is underway or there is already a problem that begins to materialize.

So that's the distinction that I think that we would all wrestle with.

The CHAIRMAN. OK.

Senator Murkowski.

Senator MURKOWSKI. Let me just follow on to that. Because it was my understanding that OK, we're in agreement that when we're talking about the imminent threats it's DOE that has that authority. They don't need to wait for anyone here.

But with the less time sensitive vulnerabilities this is where FERC has that jurisdiction. But you have that stakeholder process with ERO under section 215 that says the stakeholders go first. So the concern that has been expressed and I'm not quite sure whether it was intentional, whether it was drafting error, where we are.

But what I understand has happened with this. With the text that we're dealing with is that we may be in a situation here where FERC is able to bypass that stakeholder process with—which is not the intention. FERC could actually bypass and then effectively direct what the standards may be for—at this local level which I don't think is what we intended it to do.

So the question then becomes do we need to clarify this within the draft language so that we do not effectively allow for that bypass. That it is clear that that stakeholder process has the authority to go first, if you will. Do we need to resolve within the language this discrepancy? Because it sounds like the chairman and I are both a little bit foggy on what it actually does. It sounds like a pretty critical piece of what we're trying to resolve here.

Mr. Cauley.

Mr. CAULEY. I think there could be some clarification as I had suggested in my testimony. I think the Commission has authority today to direct us to do a very specific standard and achieve a very specific outcome. If similar language is sort of repeated in this new legislation I think it would be very beneficial if it did provide for the Commission to give us a specific objective, a problem we're trying to solve and give an opportunity for the process to work.

One of the difficulties I see with having a vulnerability section separately is the line between what we're calling vulnerabilities and threats is a very nebulous line. Vulnerabilities can come out today. A premise be made that this is a vulnerability we need to solve in a week in the area of safety and reliability doing standards fast is not usually one of my first objectives.

My first objective is to get it right and solve a problem. I think that carries over to nuclear safety, airline safety. It's not about being fast.

That's where I suggest that our ability to issue a mandatory emergency directive whether it be for a vulnerability that has now just popped up or an imminent known threat coming in from an intelligence agency. I think we need to strengthen our ability to get those directives and immediate actions out and have them have teeth and have some enforceability with that. So——

Senator MURKOWSKI. So are you suggesting that we should not have this bifurcation between the vulnerability and the imminent threat?

Mr. CAULEY. I think it's an artificial one to be honest. I think to the extent that a vulnerability is an enduring vulnerability like a solar magnetic disturbance is. It's here this week. It's here next week. It's going to be here 10 years from now. That should be handled through our standards process.

But the emergent dynamic issues that are coming up whether you call it a threat or vulnerability need some faster mechanism to respond to. I think that would be more appropriately handled through directives and actions in a, sort of in a near term basis with consultation from the entities that have to follow those requirements.

Senator MURKOWSKI. Mr. McClelland.

Mr. MCCLELLAND. There is a bifurcation in the bill between imminent danger which is a threat and then vulnerability that exposes an imminent danger. So for instance, Aurora although it was demonstrated in a laboratory there was never any intelligence that anyone planned to use it. So it would fall under a vulnerability per say.

So the bifurcation once we acknowledge the bifurcation, I personally saw it as 3 levels.

One would be the routine standards development process.

The second would be a measure to address a vulnerability through the ERO and the stakeholder process.

A third which would be an extraordinary level which would be something that needed to be done immediately that could not result in a standard. A good example would be say, distribution systems. There are no—the jurisdiction of the ERO does not extend over distribution systems. In that regard I personally thought it may be some sort of a targeted vulnerability that may be temporary in nature to address a specific issue.

Without that vulnerability though, a personal perspective is that the cyber security would be extremely difficult to prove imminent danger. There would be no Federal agency that has the ability, be it FERC, DOE, DHS or anyone that would have the ability to trust but verify to compel action and make certain that that action is taken. So from, again from a perspective, the vulnerability in the manner in the layers that I represented, I thought would be adequate, somewhat extraordinary, but adequate to address any cyber security issues.

Senator MURKOWSKI. Thank you, Mr. Chairman.

Mr. Owens, you're shaking your head. I actually had a question for you about the NERC alerts not being legally enforceable. It was Mr. Cauley. You recognize that as a gap. I'd like that addressed.

But I recognize that Senator Udall is here. Do you mind if I just finish out my question?

Senator UDALL. Go right ahead. Sure.

Senator MURKOWSKI. I have been running over the clock for the past 2 hearings.

The CHAIRMAN. Go right ahead.

Senator MURKOWSKI. I'm very conscious of that.

Mr. Owens.

Mr. OWENS. I think we are making it far too complicated.

Senator MURKOWSKI. I agree. It's getting tougher instead of easier.

Mr. OWENS. Let me just try to be very simplistic in explaining this. One side we have imminent threats. The other side we have assets that create a vulnerability where it could lead to a cyber breach that could be very disruptive to our society.

On the imminent threat side I think all the panelists agree that it requires an agency that has intelligence about the threat working with other Federal agencies and the industry to be decisive. So irrespective of jurisdictional boundaries, it's irrelevant. We're trying to do something to protect our national security.

So let's do it. So that's imminent. You got to act quickly. You got to act decisively. Let's do it. But let's make sure that folks that operate the systems are involved in the decisionmaking. So we make the right decisions, not a decision that's going to lead to unwarranted circumstances.

The second area are we have some assets that were evolving, that are evolving that now pose potential cyber risk. Some of those assets are critical. Some of those assets are not critical.

The critical assets we want to make sure that those critical assets are identified. We want to make sure that the government agencies and industry can work closely together. To make sure that we continue to have those assets secure so they remove that potential cyber risk.

The question becomes who has that responsibility. Should the Federal Energy Regulatory Commission have that responsibility exclusively on over all these critical cyber assets or should it be acknowledged that the States have a vital role too? What I'm saying is the States have a vital role to the degree that some of those critical assets are suggesting that they can lead to an imminent threat. The question becomes should the Federal Government act decisively to deal with that.

I don't have a difficulty with that. The difficulty I have is if the Federal Government, FERC, decides they have the solution only and they seek to operate and deal with that solution without having States involved and without having the industry involved. That's what the problem is.

No single Federal agency has the wherewithal to know all aspects of the system and how to correct it. It requires vertical and horizontal communication and coordination. That's where I have the difficulty with what Mr. McClelland was saying.

Senator MURKOWSKI. I appreciate that. I think you've laid it out cleanly. I wish it was that neat.

Can you comment on the enforceability of the alerts and whether or not that is a gap that needs to be addressed?

Mr. OWENS. I think Mr. Cauley is correct that NERC has a series of alerts. There are alerts that are advisory. There are alerts that require immediate action by the industry.

He said, and I would agree with him to the degree that there is an action that needs to be taken he needs to be able to be decisive in that. But he also said you need to have industry inputs. So I wouldn't quarrel with him on that.

As long as industry is involved we understand what he sees. We share his corrective actions then I think it is appropriate that we respond appropriately.

Senator MURKOWSKI. Thank you, Mr. Chairman. Thank you all.

The CHAIRMAN. Senator Udall.

Senator UDALL. This is getting interesting. I decline to defer to the Senator from Alaska for continued line of questions and answers here.

[Laughter.]

Senator UDALL. But this is, I think, why we're holding this hearing. This is very helpful. I appreciate the passion that's being displayed.

I did want to make a comment. I know Senator Burr talked at some length about the smart grid. I don't want to take all of my time.

But I would ask for answers now. But I would ask the panelists if you would in your follow on answers to questions. Define the smart grid for us.

I think we all talk about the smart grid, but I think it's in the eye of the beholder, and we need to do a better job explaining to the public what the smart grid is. We need to know as policymakers what we mean by the term, the smart grid.

[The information referred to follows:]

The digital computing, communications, and information technologies that are transforming other areas of the economy are now being applied to the electric system to improve performance and create a "smarter" grid. As described in the 2009 Smart Grid System Report prepared by DOE, a smart grid uses digital technology to improve the reliability, security, and efficiency of the electric system. New smart grid functions can be implemented throughout the system, from generation through the transmission and distribution systems and all the way to consumers. System operations will be enhanced as a growing number of distributed generation and storage resources are deployed and participating customers are able to adjust their load in response to system operating signals.

Smart grid technologies provide a secure and reliable electricity infrastructure with the following characteristics[1]:

(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.

(2) Dynamic optimization of grid operations and resources, with full cyber-security.

(3) Deployment and integration of distributed resources and generation, including renewable resources.

(4) Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.

(5) Deployment of "smart" technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.

(6) Integration of "smart" appliances and consumer devices.

(7) Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.

(8) Provision to consumers of timely information and control options.

(9) Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.

(10) Identification and lowering of unreasonable or unnecessary barriers to adoption of smart grid technologies, practices, and services.

[1] Energy Independence and Security Act of 2007, Section XIII

Senator UDALL. Secretary Hoffman, maybe I can turn to you again. We've talked a lot about cyber threats here today. There's certainly physical threats to the grid. Do you agree that that's a vulnerability we have to consider? Could the draft bill be improved to address the potential of physical threats to the grid?

Ms. HOFFMAN. The physical threats exists, and I think they've always existed. Because they are more familiar we have processes in place to address them. I think the higher urgency is trying to find a method for addressing the cyber threats.

So from my perspective the more urgent issue is actually finding a compromise among interested parties on cyber legislation so that we can better address the cyber issues that are out there.

Senator UDALL. Anybody else care to comment?

Mr. MCCLELLAND. Yes. Actually I can tie that to your smart grid question too, Senator, in that as the smart grid is deployed, smart grids become all things to all people. But assuming that it's a 2 way communication from the meters at the lowest level through perhaps communication back to the generators and central dispatch, the physical vulnerabilities also increase with the smart grid.

Good old fashioned electromechanical meters are impervious to EMP strikes or EMP events. However, intentional electromagnetic interference device, a hand held device would have a profound effect, could have a profound effect on smart grid meters. So physical also plays into where the grid is going and how the grid is evolving.

Senator UDALL. Anybody else care to comment?

Mr. CAULEY. I would just say I am concerned about physical security as well from a real world sense of what could happen bad to the grid. I think to Senator Murkowski's view. The more comprehensive and holistically we can look at this. I think the more effective legislation will be. Because we have to deal with what are the priorities. What's the next most important thing we can invest in?

So I think to have things where we can balance between physical and cyber and say, what are the real world things that can happen? What would the consequences be? I would prefer a, sort of, a more comprehensive and more holistic view.

Mr. OWENS. I would echo what Mr. Cauley just said. I would just expand it just a little bit. We're modernizing the grid. I don't know what smart grid is either. Even though I have responsibility for the industry for dealing with that it's an evolutionary, modernization of the overall grid or another way to say it we're digitizing the grid.

If we're digitizing the grid it suggests that there are a tremendous set of new challenges with respect to cyber security. It also says we've got a lot of new players. We're going to put in a lot of different kinds of equipment.

So it suggests that we need a high standard for that equipment. That equipment must be authenticated that it is cyber secure. It seems to me and this whole area is evolving so vendors, manufacturers, utilities, regulators. Those who have the responsibility for protecting the integrity of the grid, we all have to understand the language. We all have to make cyber security a top priority.

Senator UDALL. Mr. Tedeschi, do you—would you have any comments? You're the wise man at the table as the scientist among us.

Mr. TEDESCHI. I would just offer up, Senator, that there's a broad spectrum of threats out there that are real that should be considered. Cyber is certainly at the top of the list. The probability from a risk perspective is 1.0 that those threats are happening every day.

But it would be wise to consider a broader set of threats, not just EMP, but also physical attack threats, car bombs, standoff weapons, that sort of thing. There is—there are security systems around a lot of these facilities. There's standoffs. There are inherent security hardness levels to them.

But I think the owners of the utilities, Mr. Cauley, got it just right. That they understand their operations, the effects that can occur from the variety of threats and there are links into those who have additional intelligence information, if you will, that could be brought to bear that they can be aware of to factor into decisions on where to provide security, etcetera. So there's a good link, I think, into this world.

But don't forget about the other threats especially car bombs, explosive type threats, electromagnetic pulse. We haven't really touched on even unintentional electromagnetic interference from other high frequency sources like cell phones, TV transmissions, radars, that can have an adverse effect on the operation of some of the smart grid technology. It is new technology. It can be sensitive to a broad variety of electromagnetic threats not just handheld devices or nuclear EMP.

So understanding how that technology will operate in today's broad threat space within America would pay dividends long term in terms of any hardness that might be invoked.

Senator UDALL. If the chairman would indulge me, I'll just throw out a final question. Maybe a couple of you could comment and then the rest could comment for the record. I think Senator Hoeven talked a bit about Stuxnet. There's also the Aurora event.

I'm curious if some of you would briefly respond to the significance of those 2 events that we're aware of among others.

Mr. CAULEY. I would just say they're both very real. They're very real risks. Aurora, we recognized a couple years ago has the risk of damaging equipment.

One thing that we were able to do a little over a year ago is to work with the intelligence community to grasp the details of what the actual threat is, what the vulnerability is and how to fix it. So we were able to translate that into information out to industry. So I think we've got, at this point, a very high response rate in terms of addressing it.

It was real. But I think the awareness level in the last 12 months has really increased. I think the actions that have taken place.

The Stuxnet is similar. It wasn't there if you look beyond a year ago it wasn't there. Now all of sudden it's here. It's real. I think we got the information out to the industry. They took the actions to install the patches and blocks to keep that from penetrating our control systems.

So the answer is, I think, they're very real. They're very scary. They can each do damage to our grid. But I think we just have to

take the protective measures that we've been doing to make sure it doesn't happen.

But that really describes the nature of this business. Because next week, there's going to be another one that we don't know about yet. We have to keep—it's more about having the mechanisms in process to adapt and keep fixing and learning then it is to have solved this problem once.

Senator UDALL. The rest of you respond for the record. I do not want to abuse the chairman's forbearance. So thank you again for being here.

[The information referred to follows:]

The significance of Aurora and Stuxnet includes the demonstrated ability to target industrial control systems, the difficulty in identifying the attacker, the difficulty in defending against zero-day attacks, and the demonstrated ability to conduct cyber-physical, or blended attacks. The risk to the power system has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system, and cost-saving requirements have allowed some inherent physical redundancy within the system to be reduced. The specific concern with respect to these threats is the targeting of multiple key nodes on the system that, if damaged, destroyed, or interrupted in a coordinated fashion, could bring the system outside the protection provided by traditional planning and operating criteria. Such an attack would behave very differently than traditional risks to the system in that an intelligent attacker could mount an attack, as in the case of Aurora or Stuxnet, that would manipulate assets, provide misleading information to system operators attempting to address the issue, or destroy equipment.

While no such attack has occurred on the North American electric systems infrastructure to date, Stuxnet demonstrated the ability and desire to target specific components of an industrial control system. The attack was so specific in its use of industrial control systems, that any remaining skeptics should be convinced of the abilities and intent of intelligent attackers to target industrial control systems. As in most cyber attacks, timely attribution remains difficult. The ability to mask the real identity of the attacker is often a concern, and it often takes an extended period of time to make a final determination and prosecute or take other appropriate action. The originators of Stuxnet remain unknown, while a similar case could be made for attackers that might choose to exploit an Aurora-type vulnerability. Most of the developed world uses commercial software to prevent cyber attacks. The use of zero-day vulnerabilities and the USB drive delivery method for Stuxnet showed the inadequacy of current anti-virus, intrusion detection, and firewall applications to prevent unauthorized access to networks. Finally both Aurora and Stuxnet demonstrated the ability of cyber attacks to cause physical effects. Such an attack, although never experienced in North America, could damage or destroy key system components, significantly degrade system operating conditions, and, in extreme cases, result in prolonged outages to large parts of the system.

The interconnected and interdependent nature of the electric systems infrastructure requires that risk management actions be consistently and systematically applied across the entire system to be effective. The magnitude of such an effort should not be underestimated. The North American bulk power system is comprised of more than 200,000 miles of high-voltage transmission lines, thousands of generation plants, and millions of digital controls. More than 1,800 entities own and operate portions of the system, with thousands more involved in the operation of distribution networks across North America. These entities range in size from large investor-owned utilities with over 20,000 employees to small cooperatives with only ten. The systems and facilities comprising the larger system have differing configurations, design schemes, and operational concerns. Any mitigation on such a system is complex and expensive, and should be carefully planned and coordinated between the stakeholders and asset owners and operators.

The Department has supported the North American Electricity Reliability Corporation (NERC), the energy sector and other sectors, and other government departments and agencies Department of Defense efforts to mitigate the Aurora vulnerability and Stuxnet and other threats through information sharing and technology development. In addition, recognizing that Aurora and Stuxnet are just two examples in a larger threat environment, DOE, in coordination with the National Institute for Standards and Technology, NERC, and the Department of Homeland Security, is leading a public-private collaboration to develop a risk management process guideline to provide a consistent, repeatable, and adaptable process for the electric

sector, and enable organizations to proactively manage cybersecurity risk. This collaboration will build upon existing guidance and requirements to develop a flexible risk management process tuned to the diverse missions, equipment, and business needs of the electric sector and to bridge the divide between security for industrial control systems and information technology.

The CHAIRMAN. Let me just ask one final issue here, Mr. Cauley. Your organization, NERC, is a private membership organization. I'm right about that, am I not?

Mr. CAULEY. That's correct.

The CHAIRMAN. If we were to give NERC jurisdiction over distribution facilities would, in your view, should that include the ability to levy fines or penalties on companies that are not members of your organization?

Mr. CAULEY. Mr. Chairman, we actually can enforce standards and levy fines today on entities who are not members of our organization. So membership only gives us, gives a company the ability to participate in the governance. Vote on our directors and so on.

But our authority for our mandatory standards applies to 1,900 companies whether they're members or not. That authority came from—legislation.

The CHAIRMAN. You levy those fines? FERC doesn't.

Mr. CAULEY. We levy them. But the FERC approves them in all cases. So they have the oversight. They're the final approval authority.

But we have the operatives in the field that do the investigations and determine appropriate penalties and submit them to the Commission for approval.

The CHAIRMAN. Did you have any thought on this?

Mr. CAULEY. But the question—your first question was whether—if it includes distribution would that work? I'm very hopeful that if the legislation does include distribution, that it would be very limited to issues of national level interest and security. Not totally usurp the right of the States to manage and the distribution level.

But to the extent that that authority was granted to FERC I think it would be—make sense since NERC also is a national—looking at the national interest to have a similar alignment with that authority.

The CHAIRMAN. Mr. McClelland, did you have a thought?

Mr. MCCLELLAND. Yes. The Commission has a full range of authority. It has a review of the standards. It has enforcement.

Then it also has it's delegated the fee authority to the ERO to be able to levy those fines. Although they still come back to the Commission for approval. In addition we have ALJs and we have settlement processes. Then if someone doesn't like a Commission decision they could always take us to court.

So there is an iterative process with the Commission on every order that it issues. The ability to enforce a Commission rule is something that, as a regulator, that the Commission is completely comfortable with.

The CHAIRMAN. OK. Senator Murkowski, did you have additional questions?

Senator MURKOWSKI. I do not, Mr. Chairman.

The CHAIRMAN. Thank you all. This has been a useful hearing. I appreciate it.

[Whereupon, at 11:24 a.m., the hearing was adjourned.]

APPENDIX

RESPONSES TO ADDITIONAL QUESTIONS

RESPONSES OF GERRY CAULEY TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. In February, the Department of Energy launched an open collaboration with the National Institute of Standards and Technology and the North American Electric Reliability Corporation to "develop a cyber security risk management process guideline for the electric sector." Could you describe the objectives of this collaboration and how its work will filter into the NERC standards development and approval processes?

Answer. The Risk Management Process (RMP) is a public-private collaboration to develop a cybersecurity risk management guideline that enables organizations to proactively manage risk in the diverse electrical environment that exists in North America. The evolution of smart grid technology increases the electricity sector's cybersecurity risk exposure, emphasizing the need for owners and operators to employ consistent, measurable, and adaptable processes for electricity generation, transmission, distribution, retail operations, energy service providers, as well as situation awareness. Additionally, the differing jurisdictions—NERC for the North American bulk power system (BPS), States and municipalities for the distribution grid, working with the owners and operators of the grid—require a comprehensive yet flexible approach to managing risk. This effort is led by the Department of Energy (DOE) in coordination with the National Institute of Standards and Technology (NIST) and NERC, and with the collaboration of subject matter expert representatives from across the public and private sectors. DOE plans to publish these industry-wide risk management guidelines in 2011, which are intended to complement, but not replace or supersede, the current Critical Infrastructure Protection (CIP) Standards. Objectives for this collaboration include:

- Support the unique needs of the diverse utilities and other stakeholders participating in the North American electric grid with an end-to-end perspective that includes generation, transmission, distribution, retail, energy service providers and wide area situation awareness (e.g., Phasor Measurement Unit or PMU networks).
- Provide guidance in applying cybersecurity measures to the control systems and information technologies used throughout the electric grid.
- Provide guidance for an integrated organization-wide approach to managing those cybersecurity risks pertinent to operations, assets, data, personnel, and the Nation as the existing electric grid is transitioned to a smart grid.
- Leverage risk management and cybersecurity experiences and practices among the electric grid stakeholders including the risk management guidelines (NIST Special Publications, i.e., NIST 800-39; and NERC CIP Standards) and lessons learned within the Federal Government.
- Recommend implementation guidelines that apply the RMP to electric grid domains and to unique electric grid components, such as control systems.

NERC expects there will be a phased implementation of the guidelines, starting with host utilities and vendors. NERC expects to refine the practices through these demonstration projects. As the practices are demonstrated to be effective, NERC will consider whether some subsets of the practices are appropriate for inclusion in the reliability standards.

Question 2. The Discussion Draft creates a process to address cyber security vulnerabilities affecting critical electric infrastructure. The Discussion Draft left open the question of the maximum number of days FERC should have to determine whether the existing set of reliability standards are adequate to protect this infrastructure from cyber security vulnerabilities. Assuming that FERC identified a specific deficiency in the existing set of reliability standards, do you have an opinion as to how long, in days, FERC should have to make this determination? How long

should NERC have, in days, to develop standards in response to a FERC directive to address specifically-identified cyber security vulnerabilities?

Answer. As noted in my testimony, NERC does not believe the vulnerabilities section is needed. In response to this question concerning the discussion draft, NERC would defer to FERC with respect to the timeframe for FERC's determination whether existing reliability standards are adequate to protect critical electric infrastructure from cybersecurity vulnerabilities, except that the timeframe must be sufficient to allow for notice to and consultation with stakeholders, including Canadian authorities. Such consultation is essential to provide a basis for a finding that reliability standards, or other actions taken by the electric reliability organization (ERO), are inadequate or that a specific deficiency exists.

The appropriate timeframe for NERC to respond to a FERC directive to address specifically identified cybersecurity vulnerabilities will vary depending on whether specific actionable information about the vulnerability is made available to NERC and stakeholders. It will also vary depending on the approach determined by NERC to be the most effective in responding to such a directive. As discussed during the hearing, not all vulnerabilities can or should be addressed by a reliability standard. NERC has other tools at its disposal through its Alert system to address cybersecurity vulnerabilities. In addition, the legislation should authorize a mandatory and enforceable means for NERC to address cybersecurity vulnerabilities identified by FERC in addition to the use of reliability standards. One way to do this would be to authorize NERC to issue "Mandatory Directives," as discussed in response to Q. 7 below. In the case where a reliability standard is required to address an identified vulnerability, NERC should have 180 days to develop a response. The Mandatory Directives could be issued in much shorter time frame, measured in days or weeks.

Question 3. NERC submitted eight proposed cybersecurity standards, known as the Critical Infrastructure Protection (CIP) standards, to FERC for approval under section 215. FERC approved those standards in 2008 but directed NERC to make certain revisions. As I understand it, NERC continues to work on those revisions and plans to submit them to FERC somewhere in 2012. If submitted in 2012, development and approval of the first set of cybersecurity standards will have lasted around 6 years. Why has this process lasted this long?

Answer. The Reliability Standards development process is an iterative process of continuing improvement. NERC's first set of CIP standards was approved by FERC in January 2008. NERC has worked with industry, consumer representatives and regulators to strengthen the CIP Reliability Standards, and also to respond to specific directives from FERC. While this process is occurring, mandatory and enforceable cybersecurity standards have been in place and have provided important protections for the bulk power system. The need to respond to FERC directives has necessarily influenced the direction and timing of the CIP standards development process. The second set of CIP standards addressed certain high-priority directives from FERC; FERC approved that second set in September 2009. FERC's September 2009 order included new directives and gave NERC 90 days to comply. NERC filed the third version of the CIP standards in December 2009, and FERC approved that third set in March 2010.

The most recent revision to the CIP Reliability Standards—CIP-002 Version 4—was approved by the NERC stakeholders on December 31st, 2010; approved by the NERC Board of Trustees on January 24, 2011 and submitted to the Commission for approval on February 10, 2011. Work continues on further improvements to the standards, including responses to remaining Commission directives, and it is these further enhanced standards that will be submitted to the Commission in 2012.

Question 4. Can you describe how NERC's newly-approved procedures for developing a reliability standard on an expedited basis differ from the existing development procedures? How would expedited procedures make it easier for NERC to address cyber security vulnerabilities?

Answer. The new procedures approved by FERC in September 2010 provide for developing a reliability standard on an expedited basis. Key differences from the traditional standards development procedures are in the areas of confidentiality of information; use of pre-identified technical experts for standards drafting; and process streamlining.

Confidentiality

The expedited process contains procedures that provide protection of sensitive information affecting national security. The traditional procedures do not contain similar protections.

The new procedures limit the individuals who may serve on drafting teams to those who have been pre-screened for their expertise and willingness to work under strict security and confidentiality rules, and require drafting teams to work under

strict security and confidentiality rules. Sensitive information is further protected by limiting distribution of draft standards. In contrast to the general procedures, the new procedures do not require public posting of draft standards.

Technical expertise

The new procedures require formation of a Standard Drafting Team from a list of pre-identified technical experts. This provides for the necessary diversity of expertise and industry perspectives to develop a technically sound standard that can quickly be finalized and approved. Cybersecurity involves every owner, operator and user of the bulk power system—having a diverse view when crafting the language of a standard is essential. The expedited procedures assure that the Standard Drafting Team will have the collective knowledge and expertise to develop a standard that reflects an understanding of the diverse utilities and their associated equipment configurations in the North American bulk power system.

Process streamlining

The new procedures allow the Standards Committee authority to approve a wide range of process deviations, enabling a standard to be developed in a shorter period of time. The general procedures allowed some latitude in shortening the duration of only certain process steps.

These expedited processes will enable NERC to address cybersecurity vulnerabilities through a reliability standard on a timely basis—when that is the most appropriate approach.

Question 5. In your statement, you stated that NERC was concerned that the Discussion Draft contained no requirement that FERC indentify any deficiency in existing reliability standards or a cybersecurity vulnerability for NERC to address. The Administrative Procedures Act requires agencies to give notice of either the terms or substance of the proposed rule or a description of the subjects and issues involved. Is that requirement sufficient to address this concern? If not, how would NERC propose to revise Section 224(b) of the Discussion Draft to address this concern?

Answer. The Administrative Procedure Act (APA), 5 U.S.C. 553(b), which requires publication for comment of a general notice of proposed rulemaking that includes "either the terms or substance of the proposed rule or a description of the subjects and issues involved," does not resolve NERC's concern. Proposed Section 224(b) (2) requires FERC to issue an "initial order," not a proposed rule. There is nothing in the legislative text that requires FERC in its order to advise the ERO of the specific vulnerability in sufficient detail so that the ERO can respond appropriately. Moreover, proposed Section 224(b)(6)(B) authorizes FERC to issue an interim final rule "without prior notice or hearing." In contrast, the provisions of Federal Power Act Section 215(d) authorize FERC to order the ERO to submit a proposed reliability standard "that addresses a specific matter."

NERC recommends that proposed Section 224(b)(2) be revised to include at the end the following:

> The Commission's order shall specify the vulnerabilities against which such standards or directives must protect, and shall appropriately balance the risks to the critical electric infrastructure associated with such cybersecurity vulnerabilities, including any regional variation in such risks, and the costs of mitigating such risks.

Note: with respect to the inclusion of "or directives" in the above language, see the discussion in response to question 7, below.

Question 6. Your testimony states that NERC is not sure that a section to address cybersecurity vulnerabilities (section 224(b)) is needed in the Discussion Draft. Does NERC believe that there should be a means of addressing cybersecurity vulnerabilities? Should this means be mandatory and enforceable? If not, how can compliance be assured and measured?

Answer. NERC believes not only that there should be a means of addressing cybersecurity vulnerabilities, but that such means already exist. NERC addresses cybersecurity vulnerabilities today through reliability standards and through its Alert system of Industry Advisories, Recommendations to Industry, and Essential Actions. Since January 2010, NERC has issued 14 critical infrastructure protection-related Alerts; these Alerts covered matters including Stuxnet and Night Dragon.

FERC also already has authority under FPA Section 215(d)(5) to order the ERO to "submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out [section 215]."

"Cybersecurity protection" is expressly included within the definition of "reliability standard" in section 215(a)(3).

There should be a mandatory and enforceable means in addition to the use of reliability standards for NERC to address cybersecurity vulnerabilities identified by FERC. One way to do this would be to authorize NERC to issue "Mandatory Directives," as discussed in response to Q. 7 below.

Question 7. Your testimony states that making "other NERC directives" legally enforceable would significantly enhance cyber security. Can you identify these "other NERC directives"? Please describe how NERC envisions using these other directives? Does NERC envision the process of enforcing these directives being overseen by FERC? Does NERC contemplate using these enforceable NERC directives to address cyber security or other reliability vulnerabilities? What due process does NERC envisions for those entities subject to these directives?

Answer. The other NERC directives referenced in my testimony would be a new category of directives that could be called "Mandatory Directives." NERC envisions using a Mandatory Directive to address cybersecurity vulnerabilities that are not appropriate to address through reliability standards. The draft legislation should be modified to include this authority. Provision should be made for expedited FERC approval of these Mandatory Directives. As is the case with reliability standards, FERC approval would be an essential step in making these Mandatory Directives enforceable.

Enforcement of these Mandatory Directives should be overseen by FERC, just as the enforcement of reliability rules by NERC today is overseen by FERC. The same due process that applies to the enforcement of reliability standards under FPA Section 215(e) should apply to the enforcement of NERC Mandatory Directives.

Question 8a. Your testimony states that NERC has issued 14 cyber security alerts since January 2010. How do these alerts differ from NERC standards? Was the alerts process filed with and approved by FERC? Can you describe, generally, the level of compliance NERC has observed with respect to these alerts? Have any users, owners, or operators of the bulk power system that failed to comply with any of the alerts? How did NERC respond to these users, owners, and operators?

Answer. Alerts differ from NERC reliability standards in that, unlike standards, the Alerts are not enforceable. Alerts are used when NERC has a need to place industry participants on formal notice of particular matters related to the reliability and security of the electric system. The Alerts are targeted, can be developed much more quickly than standards, do not involve an industry ballot, and can reach a broader audience than just those subject to reliability standards.

NERC's alerts process is set out in Rule 810 of NERC's Rules of Procedure, which FERC approved in February 2008. Alerts and Notifications are created and deployed from NERC in its role as the Electric Sector Information and Analysis Center (ES-ISAC). The ES-ISAC coordinates electric industry activities to promote critical infrastructure protection of the bulk power system in North America, as called for by Rule 1003.1 of NERC's Rules of Procedure, which FERC approved in July 2006.

NERC has had significant interaction with registered entities, most recently in response to the Aurora and Stuxnet "Recommendation to Industry" Alerts. Following the Aurora Alert, NERC hosted four informational webinars and a technical conference with more than 1,000 people participating. NERC continues to follow-up and meet directly with entity representatives, through both outreach and personal follow-up activities. A progress check webinar was held in early May that attracted more than 400 participants and another is scheduled for June. Similarly, following the Stuxnet Alert in September 2010, NERC made contact with industry entities to confirm acknowledgement of receipt of the Alert.

While the present Alerts and Notifications are neither mandatory nor legally enforceable, the Rules of Procedure do require NERC registered entities to report on the status of activities related to any Level 2 (Recommendation to Industry) or Level 3 (Essential Action) Alert.

This obligatory reporting requirement for NERC Alerts and Notifications is unique among all of the other Computer Emergency Response Teams (CERT) and critical infrastructure Information Sharing and Analysis Centers (ISAC) that do not impose a required response component.

Question 8b. Can you describe, generally, the level of compliance NERC has observed with respect to these alerts?

Answer. The responses to the Aurora and Stuxnet alerts have been very high. Regarding United States entities that were sent the Stuxnet recommendation, as of November 2010 99% of industry acknowledged receipt of the recommendation, more than 98% have developed a response to the recommendation and routed that response to their management for approval and more than 94% have received approval from management on the response they developed. Regarding the Aurora rec-

ommendation, as of January 2011, 99% of industry acknowledged receipt, 98% have responded to NERC and 96% have received management approval for their response they developed. Implementation plans are at various levels of completion. Every six months entities must update NERC on the status of their implementation plan until the implementation is complete. The next update to this status is June 13th 2011.

Question 8c. Have any users, owners, or operators of the bulk power system that failed to comply with any of the alerts?

Answer. For those entities that have been non-responsive, NERC staff follows up with phone calls discussing the recommendation, answering questions and clarifying uncertainties. In NERC's discussions with nonresponsive entities, interaction is maintained until a response is developed and all concerns are resolved and all questions are answered. In addition to phone calls and personal interaction, NERC continues to follow-up and meet directly with entity representatives, through both outreach and personal follow-up activities such as webinars and technical conferences.

Question 8d. How did NERC respond to these users, owners, and operators?

Answer. NERC entities that do not fulfill their obligation under the Rules of Procedure will receive heightened levels of NERC attention up to and including direct senior level interaction from NERC, Regional and industry leadership. NERC, the industry including CEO's, and the Regions take the NERC Alert process seriously.

Question 9. Level Three alerts are characterized as "essential action." Has NERC ever issued a Level Three alert? How does NERC compel action consistent with these alerts from among users, owners, and operators of the bulk power system?

Answer. NERC has not yet issued an "Essential Action" Alert. Although NERC cannot compel action to implement an Essential Action, NERC has every expectation that if its Board of Trustees makes a determination that certain actions are "essential to protect the reliability of the bulk power system", then users, owners and operators of the bulk power system will take appropriate actions. NERC would follow up as necessary. Essential Actions do carry a mandatory reporting obligation. A failure to report would constitute a violation of a rule adopted under the authority of FPA section 215 and could be enforced by FERC.

Question 10. You indicated that following the 1989 geomagnetic disturbance that affected Quebec the industry learned lessons and hardened a lot of equipment hardened at northern latitudes. Can you describe the lessons the industry learned after that event? How was equipment hardened? Given that the risks of geomagnetic disturbances are not a new threat to the electric sector, have utilities in other geographic areas hardened their equipment and systems against the affects of geomagnetic disturbances?

Answer. The potential impact of geomagnetic disturbance events have gained renewed attention as recent studies[1] have suggested the severity of solar storms may be greater and reach lower geographic latitudes than formerly expected. NERC and the U.S. Department of Energy identified this as a High Impact, Low Frequency event risk to bulk power system reliability in a joint report issued in April 2010.[2] Geomagnetic disturbances (GMD) can impact bulk power system reliability. The most well-known recent experience in North America was the March 13-14, 1989 geomagnetic disturbance, which led to the collapse of the Hydro Québec system in the early morning hours of March 13, 1989, lasting approximately nine hours.

System and equipment modifications that occurred in the Hydro-Québec TransÉnergie (HQT) system following the 1989 geomagnetic storm included adding series compensation elements on long-distance AC transmission lines, rebalancing their protection systems, monitoring geomagnetic induced currents (GICs) on key pathways on their system and testing the addition of blocking capacitors to transformer neutrals. Additionally, HQT developed new analyses on how GICs impact the Québec interconnection and employed new operating and planning procedures to observe GIC impacts in voltage.

One of the characteristics of transformers experiencing high levels of GICs is increased requirements for reactive power. The bulk power system, when faced with the need for large amounts of reactive power, as Hydro Québec faced with their 480 nanotesla per minute storm in 1989,[3] may react in an unplanned or unexpected manner, including break-up, islanding, or collapse. Industry investigation is needed to determine the amount and extent of disruptions that might occur. This analysis includes determination of transformer characteristics to identify the most affected

[1] The U.S. Federal Energy Regulation Commission and Oak Ridge National Labs issued a number of reports on Geomagnetic Storms and their impact on the bulk power system in November 2010: http://www.ornl.gov/sci/ees/etsd/pes/ferc_emp_gic.shtml

[2] The High-Impact, Low -Frequency Report can be found here: http://www.nerc.com/files/hilf.pdf

[3] http://www.nerc.com/files/1989-Quebec-Disturbance.pdf

designs as well as the most, static, dynamic and transient simulations which model the non-linear behavior of each of the interconnections in North America. Once these analyses are complete, appropriate and jurisdictionally acceptable solutions, including grid hardening, relaying, operational procedures and spare equipment could be determined to maintain an acceptable level of reliability, given the relative risk from GMD events.

NERC's GMD Task Force recently held a workshop focused on potential mitigation approaches. A major outcome of the workshop was the realization that significant work is still required by industry and governmental organizations to improve not only solar storm forecasting and but also in developing robust modeling methods to understand how GMD events impact bulk power system equipment. Once impacts have been determined, suitable actions can then be taken by both planners and operators of the bulk power system in North America to ensure reliability of the grid. The primary deliverable from the workshop, an Industry Advisory NERC Alert on GMD[4] provides industry with suitable guidance for operational and planning actions given the knowledge available today to prepare for the effects of severe GMD on the bulk power system. NERC expects to provide incremental information as it become available.

Question 11. NERC's High Impact, Low Frequency Event Risk to the North American Bulk Power System report contemplates "re-launching" NERC's spare equipment database? Why is the spare equipment database not operational today? When was it stopped?

Answer. NERC maintains a database of spare transformers, called the Spare Equipment Database (SED), which is voluntarily populated by industry stakeholders.

SED is operational today. It is being re-launched in 2012 as a revitalized tool to provide increased coverage and give it increased visibility among stakeholders—in direct response to NERC's High Impact, Low Frequency (HILF) report[5] developed in collaboration with the Department of Energy. In 2010, based on the results of HILF roadmap developed by the Electricity Subsector Coordinating Council[6] and technical committees strategic coordinated action plan,[7] NERC initiated its SED revitalization efforts and will fund the development of an on-line data collection tool. SED will initially focus on bulk power transformers; however, other critical long-lead time equipment may be added in the future.

RESPONSES OF GERRY CAULEY TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. Through the definition of "critical electric infrastructure," the discussion draft legislation extends FERC's jurisdiction beyond the Bulk Power System to the distribution level as long as those systems or assets are "vital" to the nation's security, economy, public health or safety. In your testimony, you point out that NERC's authority as the ERO does not extend to the distribution level.

In the text, we were trying to respect the Section 215 stakeholder process—the idea being that if FERC directed the ERO to develop or modify a cyber standard to protect "critical electric infrastructure" that standard would be developed through the existing stakeholder process. It was certainly not my intent to allow FERC sole discretion to dictate standards at the local level or bypass the Section 215 process altogether. Please comment. Can you provide the Committee with clarifying language?

Answer. NERC appreciates the effort to respect the Section 215 standards development process. As I indicated in my testimony, under the current discussion draft structure, unless FERC and NERC have the same jurisdictional reach, it will be difficult to achieve the necessary collaboration and coordination that must take place if requirements applicable to the bulk power system and the distribution systems are to work together to achieve the desired outcomes. This issue arises because the definition of "critical electric infrastructure" in the discussion draft includes distribution facilities and the definition of bulk power system in section 215 does not.

---

[4] http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10-01__GMD__FINAL.pdf[4]

[5] Joint NERC and U.S. DOE report, High Impact, Low Frequency Event Risk to the North American Bulk Power System: http://www.nerc.com/files/HILF.pdf

[6] Electricity Subsector Coordinating Council report, Critical Infrastructure Strategic Roadmap: http://www.nerc.com/docs/escc/ESCC__Critical__Infrastructure__Strategic__Roadmap.pdf

[7] Technical Committee Report, Critical Infrastructure Strategic Initiatives Coordinated Action Plan: http://www.nerc.com/docs/ciscap/Critical__Infrastructure__Strategic__Initiatives__Coordinated__Action__Plan__BOT__Apprd__11-2010.pdf

As I stated during the hearing, NERC is not seeking jurisdiction over distribution, but is concerned about the language in the discussion draft that leads to a mismatch in NERC and FERC jurisdiction. If FERC is given jurisdiction over certain distribution facilities for purposes of addressing cyber vulnerabilities, then NERC believes it should have equivalent jurisdiction. NERC does not believe it is workable to try to address cyber vulnerabilities in two different places at the same time. NERC has proposed amendments to various aspects of the discussion draft in response to question 2, below, and the provisions dealing with the jurisdictional mismatch are included in those proposed amendments.

Question 2. You testified that given the constantly changing nature of vulnerabilities, not all vulnerabilities can or should be addressed by a standard. I understand that for the Aurora, Stuxnet, and Night Dragon attacks, NERC issued Alerts. Moreover, the Commission, which has the authority to order NERC to produce reliability standards, has never ordered NERC to take such action—is that correct? Can you provide the Committee with language to make these NERC Alerts legally enforceable?

Answer. It is correct that to date, FERC has not exercised its authority under FPA Section 215(d)(5) to direct NERC to produce a reliability standard to address a specific matter, although FERC has exercised that authority hundreds of times to direct NERC to make modifications to standards that NERC had filed for FERC approval. NERC suggests the following changes to the discussion draft to enable the ERO to promulgate Mandatory Directives in response to a Commission order under proposed Section 224(b) that will be mandatory and enforceable. The changes below also address NERC's concerns that, as written, proposed Section 224(b) does not expressly require FERC to identify the specific cyber securities vulnerabilities to be addressed by the ERO. In addition, these proposed changes address the mismatch in FERC and NERC jurisdiction that I discussed in response to the prior question. (Language to be added is underlined; language to be deleted is stricken through):

[Note: For printing purposes, italic represents underlined language and bold represents stricken through language.]

I. Add a new definition of "Mandatory Directive" as FPA Section 224(a)(8), to read as follows:

> *"(8) MANDATORY DIRECTIVE—An enforceable order issued by the Electric Reliability Organization to users, owners and operators of Critical Electric Infrastructure and approved by the Commission to address critical electric infrastructure cybersecurity vulnerabilities in response to a Commission order issued pursuant to subsection (b) of this section."*

II. Modify proposed Section 224(b)(2) to include Mandatory Directives, as follows:

> "(2) INITIAL ORDER—**Unless** If the Commission determines that the reliability standards *and alerts, advisories or other actions taken by the Electric Reliability Organization* **established pursuant to section 215** are *not* adequate to protect critical electric infrastructure from *specified* cybersecurity vulnerabilities within———days after the date of enactment of this section, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than———days after **the date of enactment of this section** *such Commission Order*, a proposed reliability standard, *or* a modification to a reliability standard, or a Mandatory Directive that will *address the cybersecurity vulnerabilities identified by the Commission* and **provide adequate protection of** protect critical electric infrastructure from cybersecurity vulnerabilities. *The Commission's order shall specify the vulnerabilities against which such standards or directives must protect, and shall appropriately balance the risks to the critical electric infrastructure associated with such cybersecurity vulnerabilities, including any regional variation in such risks, and the costs of mitigating such risks."*

III. Modify proposed section 224(b)(3) to include Mandatory Directives, as follows:

> "(3) SUBSEQUENT DETERMINATIONS AND ORDERS—If at any time following the issuance of the initial order under paragraph (2) the Commission determines that the reliability standards, alerts, advisories or other actions taken by the Electric Reliability Organization **established pursuant to section 215** *or Mandatory Directives issued by the Electric Reliability Organization pursuant to this section are inadequate to protect critical electric infrastructure from an identified* cybersecurity vulnerability, the Com-

mission shall order the Electric Reliability Organization to submit to the Commission, not later than 180 days after the date of the determination, a proposed reliability standard, or a modification to a reliability standard, **or** *a Mandatory Directive* that will **provide adequate** *address the cybersecurity vulnerabilities identified by the Commission and protect* **protection of** critical electric infrastructure from the cybersecurity **vulnerability** vulnerabilities. *The Commission's order shall specify the vulnerabilities against which such standards or directives must protect, and shall appropriately balance the risks to the critical electric infrastructure associated with such cybersecurity vulnerabilities, including any regional variation in such risks, and the costs of mitigating such risks.*

IV. Add a new section 224(b)(5) to provide for the development and approval of Mandatory Directives (and renumber succeeding subsections accordingly):

"(5) MANDATORY DIRECTIVES—A Mandatory Directive submitted by the Electric Reliability Organization pursuant to paragraph (2) or (3) shall be developed by the Electric Reliability Organization pursuant to procedures approved by the Commission, may apply to all users, owners and operators of Critical Electric Infrastructure as defined in this section, and shall be mandatory and enforceable as to such entities upon approval by the Commission, which shall act upon proposed Mandatory Directives on an expedited basis."

V. Add a new section 224(b)(7) to provide for enforcement of Mandatory Directives and reliability standards issued in response to Commission orders under Sections 224(b)(2) and (3) (and renumber succeeding subsections accordingly):

"(7) ENFORCEMENT——

(A) Mandatory Directives.—A Mandatory Directive approved by the Commission under this section may be enforced in the same manner as is provided for in section 215(e) for the enforcement of reliability standards approved under section 215.

(B) Certain Reliability Standards.—Reliability standards developed by the Electric Reliability Organization in response to a Commission order issued under paragraphs (b)(2) or (b)(3) of this section to protect critical electric infrastructure from an identified cybersecurity vulnerability, including reliability standards that replace an Interim Final Rule issued by the Commission under paragraph (b)(6) of this section, and approved by the Commission may be enforced in the same manner as is provided for in section 215(e) for the enforcement of reliability standards approved under section 215.

VI. Conforming changes would be made to include Mandatory Directives in the provisions regarding Interim Final Rules.

Question 3. In the vulnerabilities section of the discussion draft, we have yet to specify the timeframes for FERC's initial determination on the adequacy of reliability standards and for NERC's response to any Commission directive. In NERC's opinion, what is the appropriate amount of time for these actions?

Answer. NERC would defer to FERC with respect to the timeframe for FERC's determination whether existing reliability standards are adequate to protect critical electric infrastructure from cybersecurity vulnerabilities, except that the timeframe must be sufficient to allow for notice to and consultation with stakeholders, including Canadian authorities.

The appropriate timeframe for NERC to respond to a FERC directive to address specifically identified cybersecurity vulnerabilities will vary depending on whether specific actionable information about the vulnerability is made available to NERC and stakeholders. It will also vary depending on the nature of the approach determined by NERC to be the most effective in responding to such a directive. As discussed during the hearing, given the constantly changing nature of cybersecurity vulnerabilities, not all vulnerabilities can or should be addressed by a reliability standard. NERC has other tools at its disposal through its Alert system in addition to reliability standards to address cybersecurity vulnerabilities. The legislation should expressly recognize that the response to a cybersecurity vulnerability identified by the Commission may take the form of an alert, advisory or other action by the ERO. Such NERC directives can be issued very quickly, in some cases in as little as a day to several weeks, depending on the specific nature of the vulnerability. In the case where a reliability standard is required to address a vulnerability, NERC should have 180 days to develop a response.

Question 4. Do you read the discussion draft as allowing both FERC and DOE to develop different lists of critical assets? If so, can you provide clarifying language to the Committee?

Answer. The composition of the list of critical assets is vital to assuring that the appropriate owners, operators and users of critical electric infrastructure are able to receive communications affecting their assets and are aware of their obligations. NERC has itemized "bright line" criteria for the identification of critical assets as part of the most recent revision to the CIP Reliability Standards, which was submitted to the Commission for approval in February.

Because the discussion draft does not require consultation or coordination between FERC and DOE in the identification of critical electric infrastructure, there is the potential that different lists of critical assets could be identified. At a minimum, DOE and FERC should coordinate in the preparation of assets lists and use common criteria in defining critical electric infrastructure. Suggested language to accomplish this follows:

> Amend the definition of critical electric infrastructure in proposed FPA Section 224(a)(1) to add the following at the end:
>
> > The Commission and the Secretary shall coordinate in the identification of critical electric infrastructure systems and assets.

Question 5. What is the nature of NERC? Is your organization a purely private entity? How does your membership work? How many entities are on your Compliance Registry and are they all NERC members? Finally, please specify your enforcement/penalty authority.

Answer. NERC is a private, non-profit corporation governed by an independent board of trustees. By statute and NERC's bylaws, the independent trustees can have no financial or business interest in the users, owners, and operators of the bulk power system who are subject to NERC's standards. NERC's membership includes large and small electricity consumers, government representatives, municipalities, cooperatives, independent power producers, investor owned utilities, independent transmission system operators and federal power marketing agencies, such as TVA and Bonneville Power Administration and the eight regional entities. Due to the international nature and electrical properties of the bulk power system, NERC's membership also includes Canadian entities.

NERC is a non-governmental entity that has been certified by the Federal Energy Regulatory Commission as the "electric reliability organization" for the U.S. and has been delegated certain powers pursuant to FPA section 215(c)(2).

Membership in NERC is open to all entities with an interest in the reliability of the bulk power system of North America. Membership in NERC is free of charge. As of May 16, 2011, NERC has 729 members. NERC's members fall into the following sectors:

- Investor-owned utility
- State or municipal utility
- Cooperative utility
- Federal or provincial utility/power marketing administrator
- Transmission-dependent utility
- Merchant electricity generator
- Electricity marketer
- Large end-use electricity customer
- Small end-use electricity customer
- Independent system operator/regional transmission organization
- Regional Entity
- Government representative

The NERC Compliance Registry is separate from the NERC membership list and consists of users, owners and operators of the bulk power system. The entities included on the compliance registry are the ones obligated to comply with NERC's mandatory reliability standards. Entities included on the NERC Compliance Registry in many cases are, but are not required to be, members of NERC. As of May 16, 2011, 1,923 entities were listed on the NERC Compliance Registry.

NERC's authority as the ERO to enforce reliability standards is established in FPA section 215(e). Section 400 of NERC's Rules of Procedure, which have been approved by FERC, set forth the NERC Compliance Enforcement Program.[8] NERC

[8] NERC's Rules of Procedure are available at: http://www.nerc.com/files/NERC__Rules__of__Procedure__EFFECTIVE__20110412.pdf.

has the authority to impose financial penalties for violation of Reliability Standards, but those penalties cannot take effect until they have been filed with FERC, with an opportunity for FERC review. FERC has ruled that NERC may impose penalties of up to $1,000,000 per violation. FPA section 215(e)(6) requires that any penalty must bear a reasonable relation to the seriousness of the violation and must take into consideration the efforts of the user, owner, or operator to remedy the violation in a timely manner.

Question 6. In your testimony, you describe several alternative methods for approving standards, including an expedited stakeholder process and a process by which the NERC Board of Trustees can approve a standard directed by FERC if there is no consensus among your members. Do you think these processes adequately address the concerns raised by the January 2011 GAO Inspector General Audit regarding the timeliness of the stakeholder process? When did these new processes become effective and have they been used to date?

Answer. The expedited stakeholder process and the process by which the NERC Board of Trustees may propose and adopt a standard in response to a FERC directive if the Board determines that the regular standards process is not being sufficiently responsive to the Commission (Rule 321 of NERC's Rules of Procedure) are, we believe, responsive to the concerns raised in the GAO Inspector General Audit. FERC approved NERC's expedited stakeholder process on February 5, 2010; it approved new Rule 321 on March 17, 2011. To date NERC has not had the occasion to use either process.

Question 7. The discussion draft defines the term "Critical Electric Infrastructure" as follows:

> . . .means systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce that, as determined by the Commission or the Secretary (as appropriate), are so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety.

To what extent are distribution assets captured in this definition?

Answer. Distribution assets are expressly captured to the extent that they are determined by DOE or FERC to meet the statutory definition of "Critical Electric Infrastructure," i.e., to the extent they are "so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety." With no clear indication of how the criteria will be applied by FERC and/or DOE in determining what distribution assets meet the statutory definition, NERC is unable to comment on the scope or magnitude of distribution assets that may be covered. If the definition is intended to cover national defense facilities or government facilities, that should be made express. I am concerned that reading the definition to cover major metropolitan areas could lead to potential conflicts with existing State and local jurisdiction and authorities.

Question 8. You have stated that you seek to transition to risk-based assessments for not just cybersecurity standards but all standard-setting. Please update the Committee on the transition. When do you expect to base cyber security standards upon risk-based assessments? In what ways will standards change after implementing risk-based assessments?

Answer. NERC is incorporating the concept of risk into all of its standards development activities. A new project prioritization process is being used to develop the Reliability Standards Development Plan. This process evaluates several different factors, but gives considerable weight to the "reliability risk" that a project is intended to address. This risk is evaluated in both qualitative and quantitative terms—what kind of risk NERC is trying to manage, and how effectively will the proposed project manage that risk. Other areas considered in the prioritization include regulatory drivers, coordination and logistics, and general experiences with the current set of standards. Each project is evaluated relative to these areas and prioritized to help NERC allocate its resources. The risk analysis drives NERC's three-year work plan for Standards Development.

Additionally, NERC is implementing our "Results-Based Standards" initiative. This effort uses best-practices from product development to improve the quality and effectiveness of our standards. In the "Results-Based" approach, NERC develops requirements in its standards to address specific outcomes: ensuring adequate performance, managing risk, and verifying competency. NERC requires, particularly in the CIP standards, that entities take actions to mitigate risks or to demonstrate competency prior to an event occurring. In this way, we not only evaluate how well

an entity performs, but also whether they are well-prepared. By requiring specific risk-mitigation measures, we protect against the "known" risks, and by verifying competency, we ensure that the industry has the tools and skills to make informed decisions when facing unknown risks. In the CIP field, not all contingencies can be anticipated. Resilience is required.

RESPONSES OF GERRY CAULEY TO QUESTIONS FROM SENATOR UDALL

Question 1. Has the Aurora vulnerability been effectively mitigated, and how is this verified? What is the factual basis for your answer?

Answer. NERC believes that registered entities now understand the Aurora vulnerability and are taking steps to mitigate that vulnerability within their systems. The basis for this belief is as follows:

From 2007 through 2010 NERC worked closely with federal partners on information controls which finally resulted in NERC's receiving authorization to share with industry an extensive technical library designated "For Official Use Only" on NERC's various protected portals.

The availability of this technical library allowed NERC to develop and issue an Aurora "Recommendation to Industry" Alert on October 13, 2010 with more explicit information on the vulnerability and recommendations for detailed mitigation measures than was made available when the Aurora vulnerability first surfaced in 2007. This NERC Level 2 "Recommendation to Industry" carried mandatory reporting obligations in accordance with NERC Rules of Procedure (ROP) Section 810, Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions, which outlines the requirements.

The goal of the Aurora Recommendation was to disseminate vulnerability information, discuss generally-recommended mitigation measures, and gather situational awareness data critical to an industry-wide Aurora risk assessment. Work toward this goal has reduced reliability risks to the bulk power system from exposure to the Aurora vulnerability.

Through the implementation of recommended actions, based on the confidential reports received, NERC believes that the potential impact on the bulk power system from an Aurora event has been significantly reduced. Mitigation plans either have been or are in the process of being implemented, and as this process continues, the potential impact to the power system will be further reduced. Additionally, the provisioning of the technical library helped establish enhanced communication channels between NERC and the users, owners, and operators of the bulk power system and is facilitating general industry-wide awareness regarding the Aurora vulnerability.

The status of entities' continuing actions in implementing Aurora mitigation will be updated every six months in accordance with the reporting obligations in the Aurora Recommendation.

The October 2010, NERC Aurora "Recommendation to Industry" included the following questions, which NERC developed in consultation with FERC and industry subject matter experts:

1. Does your organization fully understand Aurora, especially given the new information? If not, contact NERC for assistance.
2. Has your organization assembled a project team to assess Aurora susceptibility, and/or develop Aurora mitigation recommendations based on the new information?
3. What is your plan to respond to customer inquiries regarding Aurora?
4. Has your organization taken steps to mitigate the risk of an Aurora event or attack, as both a consumer and provider of electric power?
5. Is your project plan for mitigation complete? If not, when do you expect it to be complete? Please indicate within the mitigation plan what types of assets were considered for inclusion.
6. Are your mitigation efforts complete? If not, when do you expect them to be complete?

The response to the Aurora alert has been very high. As of January 2011, 99% of industry acknowledged receipt, 98% have responded to NERC and 96% have received management approval for their response they developed. Implementation plans are at various levels of completion. Every six months entities have to update NERC on the status of their implementation plan until the implementation is complete. The next update to this status is June 13, 2011.

For those entities that have been non-responsive, NERC staff follows up with phone calls discussing the recommendation, answering questions and clarifying uncertainties. In NERC's discussions with nonresponsive entities, interaction is maintained until a response is developed and all concerns are resolved and all questions

are answered. . In addition to phone calls and personal interaction, NERC continues to follow-up and meet directly with entity representatives, through both outreach and personal follow-up activities such as webinars and technical conferences.

NERC entities that do not fulfill their obligation under the Rules of Procedure will receive heightened levels of NERC attention up to and including direct senior level interaction from NERC, Regional and industry leadership. NERC, the industry including CEO's, and the Regions take the NERC Alert process seriously.

NERC will monitor the progress of entities as they update their status every six months as required until complete. In addition NERC will execute its plans for continually closing the mitigation gap by implementing a continuous improvement action plan. NERC's action plan includes:

- Establishing a series of periodic webinars for entities to share information that will continuously inform bulk power system entities of lessons learned from continuing reviews.
- Continue to review the submitted responses and communicate with entities to solicit feedback and close gaps identified in response areas.
- As entities indicate that they have completed implementation of their mitigation plans by updating the Aurora Recommendation responses, NERC will place these entities into a category for a potential Sufficiency Review, the purpose of which is to conduct a risk-based assessment that determines an entity's ability to ensure the safe, reliable operation of the bulk power system. This review will provide additional assurance of adequate Aurora mitigation efforts.
- Continue to maintain and update the Aurora Technical Library and provide periodic updates to industry to include documents pertaining to lessons-learned, best practices and areas of concern.
- Continue to communicate with the industrial control system vendor community regarding issues and concerns discovered through Aurora mitigation activities.
- Continue to contact entities who stated that they have no Aurora-vulnerable assets to ensure adequacy of their activities.
- Maintain examples of well-designed customer outreach packages and other resources that entities make available based on the needs expressed by entities to further facilitate the sharing of information.

Question 2. Are the current spare transformer resources, including the EEI STEP program, sufficient to mitigate the transformer loss scenario presented in the Oak Ridge National Laboratory report from a 1921-level solar storm (over 300 transformers)? What is the factual basis for your answer?

Answer. NERC is studying common mode failures, such as potential increases in failure rates from geomagnetic disturbances (GMD). The number of transformers that might be required to respond to a 1921-like GMD event has yet to be determined. A detailed study of the bulk power system reaction to vulnerable transformer failures must be completed, with suitable modeling and appropriate scenarios, to understand the resulting resiliency from operational procedures and spare equipment requirements.

The electric sector has a long history of successfully managing day-to-day risk to the reliability of the bulk power system. Mitigation efforts at threatened assets, NERC's Spare Equipment Database (SED), EEI's STEP, and the many pooling/bilateral agreements that exist will support utilities in responding to and managing bulk power system reliability in the event of a significant GMD.

Generally there are a limited number of replacement spares available. Spares are typically determined by assessing the likely failure risk and balancing that against prudent, regulatory review, allocation of investment funds. Individual failure rates of bulk power system transformers (transmission auto-transformers and generation start-up) typically are low (1-1.5%). As high voltage transformers, depending on size, can range in cost from $1M to $10M+ dollars and have replacement manufacturing times of 6 to 18 months, programs such as SED, STEP and equipment pooling arrangements support industry goals to address individual failures and allow for sharing of high-cost and long lead-time electric transmission assets.

NERC would like to offer the Committee some context regarding the ORNL study.[9] FERC sponsored the study to evaluate the impacts from GMD that can cause the flow of geomagnetic induced currents (GIC) into high voltage transformers (345 kV, 500 kV and 765 kV), leading to their projected failure. A simplified bulk power system model was used to simulate GIC. Further, based on information gathered from measurements, descriptions of local geology, and validation from past observed GMDs, a zonal ground model was developed to represent the ground

[9] FERC sponsored ORNL report Meta-R-319 http://www.ornl.gov/sci/ees/etsd/pes/ferc__emp__gic.shtml.

impedances.[10] A set of GMD homogenous intensities and orientations was developed, the resulting GICs were modeled, and quasi-direct current (DC) injections into transformer ground neutrals were calculated.

Based on the results of the study, when the intensity of a homogenously modeled GMD reach 4,800 nanotesla per minute (projected as the intensity of the 1921 solar storm) at the 50 degree geomagnetic latitude in the Northern Hemisphere, nearly 1,000 high voltage transformers experienced GICs greater than 30 amps per phase and over 300 high voltage transformers experienced greater than 90 amps per phase. In these scenarios, all bulk power system lines were assumed to be in-service, a single system dispatch and loading was assumed, and the transformers experiencing the specified GIC neutral amperage were assumed to irreparably fail. The assumption depicted in the study, and reflected in FERC's testimony at the hearing, is that all transformers with GIC at or above 90 amps per phase in their neutrals, would catastrophically and simultaneously fail, causing an unrecoverable blackout for more than six months. More work is needed before one can draw that, or any, conclusion.

The contention that all high voltage transformers will catastrophically fail simultaneously for the 4,800 nanotesla/minute scenario affecting 130 million people is a simplistic view, which ignores the dynamic and system operational character of the bulk power system. This forecast assumes the dynamic characteristics of the bulk power system and its resiliency are irrelevant parameters, all transformers are equally sensitive to GIC flows, and the system will neither act nor respond when transformers experience high levels of GIC. Further, it is unclear if the intensity of the field strengths, in reality, is homogenous. Rather, the fields can be made up of a variety of structures creating local GIC flows, resulting in narrow concentrated impacts, rather than broad-scale affects. There is a danger in overreacting to worst-case scenarios. Industry organizations do take these issues seriously, but resources are limited. Over-commitment of resources to address the worst-case scenario will take resources away from addressing other, more probable risks. NERC's current work is focused on performing a realistic and responsible assessment of the impacts and priorities for mitigation, so that it is possible to balance the real risks and the costs of appropriate mitigation.

The appropriate use of the FERC study is as a screening assessment to identify those transformers that may be most vulnerable from GIC effects. The prudent next step is for additional detailed simulation of bulk power system behavior. For example, when the injected DC entering a transformer neutral reaches significant levels (e.g. 90 amps per phase), the resulting core saturation acts as a large reactor, and, therefore, demands large amounts of reactive power from the bulk power system. The reactive demand would result in voltage profile variations triggering automatic action in some cases, and operator action in others. High levels of GIC would also cause conventional current transformers to saturate, providing unreliable signals used to support system protection. Further, large quantities of harmonics would emanate from the saturated transformers, also interfering with system protection objectives. The affects of these characteristics on the bulk power system under multiple credible scenarios, loadings and system conditions must be simulated to ensure a full understanding of potential impacts.

The bulk power system, when faced with the need for large amounts of reactive power, as when Hydro Québec was faced with their 480 nanotesla per minute storm in 1989,[11] may react in an unplanned or unexpected manner, including break-up, islanding, or collapse. Industry investigation is needed to determine the amount and extent of disruptions that might occur. This analysis would include static, dynamic and transient simulations which model the non-linear behavior of each of the interconnections in North America. Once these analyses are complete, appropriate and jurisdictionally acceptable solutions, including grid hardening, relaying and spare equipment could be determined to maintain an acceptable level of reliability, given the relative risk from the GMD event.

Finally, the study was developed by FERC without industry vetting of the modeling approaches, simulation algorithms or basic data supporting the results. More assessment of the algorithms and simulation approaches with industry input is a vital next step, as addressed in testimony of Dr. William Tedeschi, Senior Scientist, Sandia National Laboratories.

Question 3. How effective has the current standards development process been in protecting against cyber and other non-cyber threats and vulnerabilities to the grid?

---

[10] Ground impedances form part of the circuit that determines GIC flows. GIC results from changes in Earth's magnetic field caused by GMD

[11] http://www.nerc.com/files/1989-Quebec-Disturbance.pdf

Is it possible to use this process supplemented with NERC's emergency standards process and the Alerts process to get the job done?

Answer. NERC's mandatory and enforceable standards have resulted in unprecedented industry-wide focus and attention to protecting the grid against cyber and non-cyber threats. It may be possible to get the job done using standards and NERC's alert and advisory system, especially if NERC's proposal for Mandatory Directives is accepted. However, some agency in the federal government should be given authority to respond to a genuine cyber emergency, because such an emergency may demand swift and widespread action of a sort not achievable by the ERO, particularly given the challenge of translating classified information to industry in a useable form.

RESPONSE OF GERRY CAULEY TO QUESTION FROM SENATOR PORTMAN

Question 1. Multiple levels of protection on the electric system have significant, additional costs, and may not be the most cost-effective means of mitigating known vulnerabilities or combating known threats. How would you recommend that determinations be made about additional security requirements that are ordered to be put in to place? Should there be a risk assessment required to determine cost-effectiveness?

Answer. Yes, there should be. I believe the reliability investment that we are promoting every day through our standards, compliance program, alerts, and other initiatives, should be driven primarily by overall value to customers and ratepayers. It is important to achieve reliability risk mitigation in a manner that balances affordability of electricity in a competitive global market with the need to ensure the reliability and security of our North American electricity infrastructure. Additional security requirements should be identified through priorities and must be driven by a clear understanding of risks and consequences, as well as the costs and benefits associated with addressing them.

In February, FERC held a technical conference to begin the discussion on the identification of priorities. The setting of priorities for NERC has to take into consideration the need to be responsive to regulatory directives from the Commission as well as priorities identified by Congress. Beyond simply discussing priorities there must be a systematic approach for analyzing risks and setting priorities going forward.

RESPONSES OF GERRY CAULEY TO QUESTIONS FROM SENATOR SHAHEEN

Question 1. There is wide agreement that our goal needs to be to prevent a cyber attack from ever being successful. But we also can't ignore the possibility that we will one day see some disruption in our infrastructure due to this kind of threat. If there was a successful attack on U.S. electrical infrastructure, how widespread could the effects be? How much would this cost the economy?

Answer. The resilience of the bulk power system in North America is well documented and while we occasionally experience isolated outages due to weather or other natural disasters, those outages are generally limited in geographic areas and rarely last for a long period of time. Coordinated physical and cyber attacks intended to disable elements of the power grid or deny electricity to specific targets, such as government or business centers, military installations, or other infrastructures differ from conventional risks in that they result from intentional actions by adversaries and are not simply random failures or acts of nature. Damage experienced during a cyber attack on a critical infrastructure like the electrical sector is difficult to quantify because there are too many variables, every potential attack is unique and most importantly, it has never happened before. However, it is difficult to imagine a scenario with the electric sector infrastructure in place today that would result in widespread outages for any significant length of time. There are several major factors that could contribute to the cost of a cyber event: actual damage to equipment, economic losses due to lack of electricity; and perhaps most importantly, the human suffering that could ensue. Damage to equipment is manageable from a cyber perspective but physical attacks on equipment such as transformers, if methodically orchestrated by a determined adversary, could result in extended outages until replacement equipment was identified, transported and installed. Any extended outage, depending upon geographic location, could result in significant economic costs and impact on the safety and well-being of citizens.

Question 2. Is there anything that can be done to limit how much damage can result from a single attack?

Answer. Yes. Critical Cyber Assets (CCA) are required to be segmented both from other system assets and each other. CCAs are incorporated into the larger Electronic Security Perimeter (ESP) that controls and identifies all access points within

utilities. As a result of this segmentation, if one ESP is compromised, other ESPs are not necessarily compromised, thus limiting any attack damage.

Limiting damage and the potential effects of a cascading environment is important to NERC and the electricity industry. Current CIP Standards contain requirements for response and recovery planning for cybersecurity incidents. For example, NERC Reliability Standard CIP-008, Incident Reporting and Response Planning, requires that the Responsible Entity develop and maintain a cybersecurity incident response plan and implement the plan in response to cybersecurity incidents. At a minimum, the cybersecurity incident response plan must address:

- Procedures to characterize and classify events as reportable cybersecurity incidents.
- Response actions, including roles and responsibilities of cybersecurity incident response teams, cybersecurity incident handling procedures, and communications plans.
- A process for reporting cybersecurity incidents to the ES-ISAC. The Responsible Entity must ensure that all reportable cybersecurity incidents are reported to the ES-ISAC either directly or through an intermediary.
- A process for updating the cybersecurity incident response plan within 30 calendar days of any changes.
- A process for ensuring that the cybersecurity incident response plan is reviewed at least annually.
- A process for ensuring the cybersecurity incident response plan is tested at least annually. Testing the cybersecurity incident response plan can range from a conducting a paper drill, to holding a full operational exercise, to responding to an actual incident.

NERC Reliability Standard CIP-009, Recovery Plans for Critical Cyber Assets, requires that the Responsible Entity create and annually review recovery plans for CCAs. At a minimum, the recovery plans must address the following:

- A definition of severity that would activate incident recovery plans.
- An annual review of exercise recovery plans.
- A process and procedure for the backup and storage of information required to successfully restore CCAs.
- Annual testing of information essential to recovery that is stored on backup media. This testing is to ensure that the information is available.

The bulk power system is highly redundant and planned with sufficient resources to accommodate unexpected loads, including a contingency/reserve margins to meet balancing and regulation needs. Redundancy plays an important role for reliability and it implies that more than one means should exist to perform a given function. In the case of a targeted attack, it is this system redundancy that will mitigate system failure and cascading effects.

Question 3. Are the possible results of a successful cyber attack incorporated into broader reliability planning?

Answer. Yes. Establishment and continued refinement of NERC's enterprise risk-based programs, policies and processes to prepare for, react to, and recover from cybersecurity vulnerabilities continue to be a high priority. NERC's Reliability Assessments and Performance Analysis Division (RAPA) is dedicated to annually assessing the adequacy of the bulk electric system in the United States and Canada and produces special assessments to assist with planning purposes. In 2010, DOE and NERC produced the High Impact, Low Frequency (HILF) Event Risk to the North American Bulk Power System report which focused on a class of rare risks with the potential to cause long-term catastrophic damage to the bulk power system. The HILF report looked at pandemic illness, coordinated cyber, physical, or blended attacks on the system, geomagnetic disturbances (GMD) caused by extreme solar weather, and the high-altitude detonation of a nuclear weapon. While some of these events have never occurred and the probability of future occurrence and impact is difficult to measure, the report identified nineteen proposals for action for government and industry to evaluate and where necessary, enhance current planning and operating practices to address these risks.

Following release of the HILF report, the Electricity Sub-Sector Coordinating Council (ESCC) developed the Critical Infrastructure Strategic Roadmap which provided a framework to address severe-impact risks, including those identified in the report. NERC staff and the leadership of the NERC technical committees (Planning, Operating, and Critical Infrastructure Protection Committees) have developed the Critical Infrastructure Strategic Initiatives (Coordinated Action Plan) to address these severe impact scenarios. The following task forces have been created to further develop this plan:

1. The Cyber Attack Task Force (CATF) is charged with considering the impact of a coordinated cyber attack on the reliable operation of the bulk power system and also identifying opportunities to enhance existing protection, resilience and recovery capabilities.

2. Physical attack scenarios are addressed in two task forces—the Severe Impact Resiliency Task Force (SIRTF) and the Spare Equipment Data Base Task Force (SEDTF). The SIRTF was formed to provide guidance and options to enhance the resilience of the bulk power system to withstand and recover from coordinated cyber and physical attacks as well as GMD.

3. The SEDTF was assigned to vet and redesign the SED, including policies and protocols for its deployment across North America. NERC has for many years (early 1980's) operated an informal transformer-based Spare Equipment Database (SED) for assisting utilities following events that exceed planned contingencies. NERC is currently reorganizing and formalizing SED to provide wider coverage among the many NERC participants and provide broader coverage of the spare transformers to be reported to the program.

4. The Geo-Magnetic Disturbance Task Force (GMDTF) was formed to identify the current capabilities, potential impacts and resiliency to GMD. The GMDTF will also identify modeling requirements to support the requisite screening and detailed study of vulnerable transformers to understand bulk power system behavior and appropriate hardening and operational requirements. In April 2011, NERC sponsored an industry workshop on responding to geo-magnetic disturbances.[12]On May 10, 2011, NERC issued an Advisory Alert to industry on the operational preparatory actions and bulk power system planning activities.[13]

RESPONSES OF DAVID K. OWENS TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. At the 2009 Committee hearing on electric cyber security, you testified that 1) consultation with industry was critical to improving cyber security and that 2) legislation should complement, not supplant, the existing reliability processes. Do you believe that the changes in today's Discussion Draft respond to your comments from last Congress? With which federal and state agencies do you coordinate on cyber security threats and vulnerabilities?

Answer. We appreciate the Committee's continued efforts on this critical issue. The Committee's "Discussion Draft" still provides significant latitude for the Federal Energy Regulatory Commission (FERC) to act unilaterally in mitigating cyber vulnerabilities. Unintended consequences of mitigation are a concern absent input from the stakeholder-driven, Electric Reliability Organization (ERO) process contemplated in §215 of the Federal Power Act.

The industry currently coordinates with law enforcement at both the state and federal level, as well as with state and Federal regulatory bodies, including FERC and the various state public utility commissions. At the Federal level we also continue to develop relationships and work with the Department of Defense, Department of Homeland Security, Department of Energy, as well as the intelligence community, senior Administration leadership, and standards bodies like the National Institute of Standards and Technology.

Question 2. Your testimony states that vulnerabilities, by their nature, offer some time to determine the best response. Do you believe that the process for addressing cyber security vulnerabilities in the Discussion Draft can be completed in sufficient time to address vulnerabilities?

Answer. Yes. In fact, we would encourage more coordination and stakeholder input, such as that outlined in §215 of the Federal Power Act.

Question 3. Your testimony highlights information sharing between government agencies and utilities as an important issue. Do you believe that this bill meets the needs of the industry in that area?

Answer. We appreciate the language in the "Discussion Draft" that requires procedures be set up for information sharing that enables the industry to implement rules or orders stemming from the legislation. While we would prefer a very explicit mandate for sharing, as well as public-private coordination and consultation in all situations that time allows, we believe the Committee took an important step by addressing information sharing in its draft.

---

[12] See agenda at http://www.nerc.com/docs/pc/gmdtf/GMD__Workshop__rev6__04.19.2011.pdf

[13] Industry Advisory, Preparing for Geo-Magnetic Disturbances, issued on May 10, 2011, http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10-01__GMD__FINAL.pdf

Question 4. You testified that industry is working with NERC to harden systems against and create redundancy in the systems to protect against the affects of solar disturbances. Can you provide an update on the general course of progress that members of your coalition are making? Does EEI believe that the power grid in the United States, or regions within it, hardened against solar-magnetic disturbances or electromagnetic pulse from man-made events?

Answer. EEI has not performed a formal survey of its members, but we are aware that a number of EEI member companies have started to purchase transformers with features that provide protections against ground induced current like those caused by solar disturbances.

In addition, EEI member companies are working with NERC to develop operational practices to mitigate risks associated with solar disturbances through its Geomagnetic Disturbance Task Force (GMDTF). In fact, on May 10, 2011, NERC issued an Industry Advisory on Preparing for Geo-Magnetic Disturbances.

http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10-01__GMD__FINAL.pdf

NERC is actively addressing a range of high-impact, low-frequency (HILF) risks to the bulk power system. These efforts are coordinated through several task forces on which EEI and EEI member companies participate, including: the GMDTF, the Spare Equipment Database Task Force, the Cyber and Physical Attack Task Force, and the Severe Impact Resilience Task Force.

The goal of these efforts is to develop models to better understand the nature and effects of Coronal Mass Ejections (CME), the vulnerabilities of equipment, bulk power system design considerations, ability to reduce the operational and real time impacts of geo-magnetic disturbances (GMD) on the bulk power system, inventory long-lead time equipment, and restoration methods. Additional information will be issued as findings from this assessment are completed.

EEI believes that efforts underway to mitigate risks associated with solar disturbances do, in fact, reduce risk. We believe, consistent with the testimony of Dr. William Tedeschi, more research is needed in this area to better understand potential impacts and identify additional effective risk mitigation strategies.

EEI believes there are residual risks associated with solar-magnetic disturbances, and that there may not be 100% protection possible against the most severe events.

Regarding electromagnetic pulse events from man-made activities, we think that it is useful to differentiate between localized effects that might be created from a portable device to create disruptive electromagnetic energy vs. potential EMP from a high-altitude nuclear weapon. A localized disruption would be handled similarly to how electric utilities currently handle significant natural disasters. For example, in the event that a tornado, flood, hurricane, or wild-fire were to cause a particular facility to be non-operational, the electric utility would initiate restoration activities and, as appropriate, migrate operations to backup facilities.

Regarding potential EMP effects resulting from the detonation of a high-altitude nuclear weapon, electric utilities rely on national defense to prevent such events from occurring.

Question 5. NERC's High Impact, Low Frequency Event Risk to the North American Bulk Power System report states that the interconnected nature of the bulk power system requires that risk management actions be consistently and systematically applied across the entire system to be effective. If there are distribution-level systems and assets that are so vital that their loss would have a debilitating impact on national security, national economic security, or national public health or safety, why shouldn't we apply risk management processes consistently and systematically to this limited set of systems and assets? Do you think each state has adequate cyber expertise and has already taken the steps needed to protect distribution facilities?

Answer. To the degree there are distribution-level systems and assets that are so vital that their loss would have a debilitating impact on national security, national economic security, or national public health or safety, they could be protected in a manner consistent with the recently released Administration proposal for critical infrastructure protection. Given the interests of the States concerning distribution-level systems, it is important to coordinate protection strategies with them.

Question 6. NERC has stated that not all vulnerabilities can or should be addressed by a standard. Do you agree? If yes, what would be the appropriate means of addressing some of these vulnerabilities? Would you support making NERC directives other than standards mandatory and enforceable?

Answer. Cyber threats and vulnerabilities evolve very quickly and oftentimes are specific to a particular entity or type of asset, but standards are designed to "standardize" procedures or processes in a more long-term, broadly applicable way. In-

stead, patches and alerts are the preferred approach for addressing rapidly-evolving, targeted threats and vulnerabilities.

In limited circumstances and with stakeholder input designed to meet a very short deadline, it could make sense for NERC alerts or directives to be mandatory and enforceable. With respect to the limited circumstances, I would suggest classifying a fourth level of alert—currently, there are three—which would provide NERC with this authority under circumstances where failure to patch the vulnerability could have particularly devastating effects. With respect to industry input, we continue to make the case that, to the best of everyone's ability, unintended consequences from mitigation need to be avoided, and having grid engineers suggesting mitigation is the most prudent way to accomplish this.

RESPONSES OF DAVID K. OWENS TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. You note that the distinction between imminent threats and less time sensitive vulnerabilities is important. I understand that EEI, along with the rest of the industry, supports new federal authority to deal with emergency threats. However, you believe vulnerabilities are already covered through the Section 215 process so additional FERC authority in this area is not necessary. Is that correct? Do you support NERC's request to make their Alerts legally enforceable?

Answer. EEI supports new federal authority to deal with emergency threats; however vulnerabilities are already covered through the Section 215 process so additional FERC authority in this area is not necessary.

Cyber threats and vulnerabilities evolve very quickly and oftentimes are specific to a particular entity or type of asset, but standards are designed to "standardize" procedures or processes in a more long-term, broadly applicable way. Instead, patches and alerts are the preferred approach for addressing rapidly-evolving, targeted threats and vulnerabilities.

In limited circumstances and with stakeholder input designed to meet a very short deadline, it could make sense for NERC alerts or directives to be mandatory and enforceable. With respect to the limited circumstances, I would suggest classifying a fourth level of alert—currently, there are three—which would provide NERC with this authority under circumstances where failure to patch the vulnerability could have particularly devastating effects. With respect to industry input, we continue to make the case that, to the best of everyone's ability, unintended consequences from mitigation need to be avoided, and having grid engineers suggesting mitigation is the most prudent way to accomplish this.

Question 2. You testified that any new government authority should be limited to covering truly critical assets—that over-inclusion of electric utility infrastructure would be counterproductive. Are you talking about allowing FERC to get down to the distribution level, even for "vital" assets? If we do allow FERC this additional authority, do you agree with NERC that the discussion draft should be amended to make sure the ERO, and the Section 215 stakeholder process, can cover this local level as well?

Answer. To the degree there are distribution-level systems and assets that are so vital that their loss would have a debilitating impact on national security, national economic security, or national public health or safety, they could be protected in a manner consistent with the recently released Administration proposal for critical infrastructure protection. Given the interests of the States concerning distribution-level systems, it is important to coordinate protection strategies with them. And, given the value of the ERO process, it is important that any FERC authority be buttressed by stakeholder input.

Question 3. In the vulnerabilities section of the discussion draft, we have yet to specify the timeframes for FERC's initial determination on the adequacy of reliability standards and for NERC's response to any Commission directive. In EEI's opinion, what is the appropriate amount of time for these actions?

Answer. It is important to balance the need for FERC to have sufficient time to review the current standards in light of known potential vulnerabilities with the need to identify those potential vulnerabilities in an expeditious manner so that NERC can begin its standards development process. Given that FERC is already familiar with the existing body of standards, having previously approved them, a period of around 120 days may be appropriate. Similarly, the time for NERC to respond must also be a balance of the need to respond to potential vulnerabilities in a prompt manner while giving the NERC standards development process a sufficient time to complete the task. Given that NERC has adopted procedures that provide for faster action in certain cases, a similar 120 period may be appropriate. FERC and NERC may have views on this issue.

Question 4. You note in your testimony that the new proposed authority for FERC to issue an "Interim Final Rule" could be done with no hearing or prior notice. The provision was written this way because the intent was for a NERC developed standard to eventually supplant the FERC Interim Rule. If the Committee fixes the discrepancy problem with NERC's ability to reach the distribution level do you still have due process concerns?

Answer. Since NERC does not have authority to develop standards for facilities used in local distribution, this effectively means FERC would be writing standards or directing operational changes for distribution facilities. Giving FERC this jurisdiction over local distribution facilities is contrary to both Section 215 and the Federal Power Act as a whole, which excludes from federal jurisdiction facilities used in the local distribution of electric energy.

However, EEI remains concerned with the provision even if distribution facilities were removed. As I pointed out in my written and oral testimony, utilities understand how their complex systems are designed and operated and "are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such exploitation, including ensuring against unintended consequences of remedial actions. It is critically important to establish a workable structure that enables the government and the private sector to work together in order to provide a more secure system for our customers." This is why it is vitally important that there be consultation and an opportunity for comment, even if expedited, before FERC could develop an "interim final" rule. An interim final rule is, in effect, "final" until replaced with another rule. Industry consultation is imperative in order to develop a solution that protects utility systems and customers. This is an integral part of the public-private partnership that the majority of witnesses at the hearing endorsed.

Question 5. The potential threat from an EMP attack or geomagnetic disturbances is not new. Given the existing knowledge of the potential for these types of disruptions, what steps have been taken to protect our grid from EMP and geomagnetic-related events? Are hardening standards in place for new products being placed onto the grid?

Answer. Although the threats posed by potential EMP effects resulting from the detonation of a high-altitude nuclear weapon are not new, the discussion of the potential for a rogue nation to launch and detonate a small number of high-altitude nuclear weapons is relatively new, and significantly different than a "cold war" discussion of "mutually assured destruction." The industry is not in the position to evaluate the threats posed by potential rogue nation(s) in this regard.

A number of electric utilities and regional transmission operators have developed operational procedures to reduce the risk to the system during elevated periods of solar disturbance activities. In addition, entities receive and evaluate solar magnetic event predictions generated by National Oceanic and Atmospheric Administration (NOAA) Space Weather Prediction Center (SWPC).

There are no uniform (standard) specifications for new transformers to mitigate ground induced currents associated with solar magnetic disturbances. Moreover, there are a number of installation specific attributes to be factored into potential designs including the characteristics of the energy to be transformed (e.g. voltage, impedance, etc.) as well as the relative resistance/conductivity or underground rock formation of the installation site.

EEI has not performed a formal survey of its members, but we are aware that a number of EEI member companies have started to purchase transformers with features that provide protections against ground induced current like those caused by solar disturbances. Although entities purchasing new transformers can designate product characteristics that may mitigate the risk of geomagnetic disturbances, they are not required to do so.

Question 6. Please describe the industry's existing Spare Transformer Sharing program. What more can be done in this area?

Answer. Please see attached STEP Overview document.*

RESPONSES OF DAVID K. OWENS TO QUESTIONS FROM SENATOR UDALL

Question 1. Has the Aurora vulnerability been effectively mitigated, and how is this verified? What is the factual basis for your answer?

Answer. On October 13, 2010, NERC issued an Alert titled:" AURORA Mitigation—Protection and Control Engineering Practices and Electronic and Physical Security Mitigation Measures."

---

* Document has been retained in committee files.

NERC required registered entities to respond to NERC regarding their mitigation status. Those entities that have not completed mitigation are required to report their status to NERC every six months until they are complete. NERC is best able to provide an answer to your question.

Question 2. Are the current spare transformer resources, including the EEI STEP program, sufficient to mitigate the transformer loss scenario presented in the Oak Ridge National Laboratory report from a 1921-level solar storm (over 300 transformers)? What is the factual basis for your answer?

Answer. The EEI STEP program is currently structured to address responding to a terrorist attack on substations and transformers, rather than a geomagnetic disturbance. Although there are spare transformers available, it is not known with certainty whether the available spares would adequately respond to the scenario envisioned in the Metatech report.

We don't have access to the assumptions, methodology or selection criteria used by Metatech, or how the conclusion regarding transformer failure was arrived at. It is our understanding that the report was not subject to scientific or industry peer review.

Question 3. How effective has the current standards development process been in protecting against cyber and other non-cyber threats and vulnerabilities to the grid? Is it possible to use this process supplemented with NERC's emergency standards process and the Alerts process to get the job done?

Answer. It's effective and improving. Yes, it's possible to get the job done as you suggest, and given the complexity of the bulk power system, it is critical to continue to actively engage owners and operators of the system as well as industry stakeholders in the development of mandatory and enforceable standards.

RESPONSE OF DAVID K. OWENS TO QUESTION FROM SENATOR PORTMAN

Question 1. Multiple levels of protection on the electric system have significant, additional costs, and may not be the most cost-effective means of mitigating known vulnerabilities or combating known threats. How would you recommend that determinations be made about additional security requirements that are ordered to be put in to place? Should there be a risk assessment required to determine cost-effectiveness?

Answer. Risk assessments should be used to prioritize threats and vulnerabilities and evaluate potential risk mitigation strategies. In a resource-constrained environment, choices will have to be made about which risks to address, and to what degree.

It is appropriate to recognize that it is simply not possible to prevent all failures. In addition to prevention, the electric utilities have demonstrated a significant resilience in response to various local and regional disasters.

RESPONSES OF JOSEPH MCCLELLAND TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. The Discussion Draft creates a process to address cyber security vulnerabilities affecting critical electric infrastructure. The Discussion Draft left open the following question: what is the maximum number of days the Federal Energy Regulatory Commission (FERC) should be granted to determine whether the existing set of reliability standards are adequate to protect this infrastructure from cyber security vulnerabilities. Can you estimate how long, in days, it might take FERC to make this determination?

Answer. I believe 120 days would be adequate for FERC to make this determination. This would include time for the Commission to issue a proposed determination, seek and consider public comments and then issue its determination.

Question 2. How long NERC should have, in days, to develop standards in response to a FERC directive to address cyber security vulnerabilities?

Answer. I believe 60 days would be adequate for NERC to develop standards in response to a FERC directive.

Question 3. Your testimony states that NERC submitted eight proposed cyber security standards, known as the Critical Infrastructure Protection (CIP) standards, to FERC for approval under section 215. Your testimony further states that FERC approved those standards in 2008 but directed NERC to make certain revisions. As I understand it, NERC continues to work on those revisions and plans to submit them to FERC somewhere in 2012. If submitted in 2012, development and approval of the first set of cyber security standards will have lasted around 6 years. Why has this process lasted this long?

Answer. The length of time it has taken for the CIP standards to be developed and implemented illustrates the potential limitations of NERC's standards develop-

ment process. Under section 215 of the Federal Power Act, the ERO's standards development process must provide for reasonable notice and opportunity for public comment, due process, openness, and balance of interests in developing reliability standards. Accordingly, NERC's standards development procedures, under which the CIP standards must be developed, allows for extensive opportunity for stakeholder participation. The NERC standards development process is intended to develop consensus on both the need for, and the substance of, the proposed standard. This results in a relatively slow process.

Question 4. Can FERC describe the advantages of having a definition of "Critical Electric Infrastructure" that is slightly more expansive than the current definition of "Bulk Power System"?

Answer. The ERO's current interpretation of the definition of bulk-power system excludes virtually all of the grid facilities in certain large cities such as New York. Moreover, the bulk-power system is statutorily defined as excluding facilities used in local distribution. Thus, the advantage of having a definition of "Critical Electric Infrastructure," as set forth in the Discussion Draft that is more expansive than the current definition of "bulk-power system," as defined in section 215(a)(1) of the Federal Power Act, is the Commission would be, for the first time, authorized to take action to mitigate cyber security vulnerabilities that involve certain critical distribution facilities and certain critical transmission facilities located in major population areas. However, the Discussion Draft includes these facilities only if their incapacity or destruction "would have a debilitating impact on national security, national economic security, or national public health or safety."

Question 5. Your testimony states that the Federal Power Act allows for some degree of discretion in defining elements of the Bulk Power System. (Your 2009 testimony made the same point.) From FERC's perspective, has progress been made to the processes of identifying critical assets? Do users, owners, and operators have the same level of discretion some two years later?

Answer. In February 2011, NERC filed a petition seeking approval of Version 4 of the CIP standards. Version 4 includes new proposed criteria to identify "critical assets" for purposes of the CIP reliability standards. This filing is currently under review by the Commission. Thus, I cannot address its merits at this time. In order to better understand the NERC Version 4 petition, particularly the number of critical cyber assets that will be identified under this revision, the Commission issued data requests to NERC, with responses due on July 11, 2011, which reflects an extension of time requested by NERC. Currently, users, owners and operators essentially have the same discretion as to whether their facilities fall under the CIP standards because there has been no change in method of identifying critical cyber assets in the CIP Standards that are currently in-effect.

Question 6. Do you think every State has adequate cyber expertise to protect distribution-level systems and assets that that are so vital that their loss would have a debilitating impact on national security, national economic security, or national public health or safety?

Answer. I do not know whether every State has adequate cyber expertise to protect these distribution-level systems and assets. However, expertise and coordination at the state level would have to include the knowledge of how cyber security vulnerabilities on the distribution-level systems and assets, along with their associated connectivity, could have a debilitating impact on the bulk-power system as well as on national security, national economic security, or national public health or safety.

Question 7. NERC indicated that industry learned lessons and hardened a lot of equipment following the 1989 geomagnetic disturbance that affected Quebec. Does FERC believe that the power grid in the United States, or regions within it, hardened against solar-magnetic disturbances or electromagnetic pulse from man-made events?

Answer. I am not aware of information showing that the power grid has been hardened to withstand a geomagnetic disturbance or an EMP event. Steps taken after the 1989 geomagnetic event are principally operational in nature. Further, according to the NERC—DOE High Impact, Low Frequency Event Risk to the North American Bulk Power System Summary Report (June 2010), the procedures put in place after the 1989 geomagnetic event were not designed for the extreme geomagnetically induced current (GIC) levels considered in the NERC-DOE study. The recommended actions in the NERC-DOE study include monitoring of NOAA alerts, reducing loading on critical transmission facilities, increasing generation reserves, and deferring or discontinuing maintenance. Some utilities have readjusted protection systems to be more tolerant of harmonic currents in order to reduce the probability of undesirable operation under GIC conditions. However, none of these actions reduce or prohibit the flow of GIC on the system and are not considered to

be hardening of equipment to protect against an EMP event. Although we have received information about a few utilities that have attempted to harden some individual elements within their systems against either a solar magnetic disturbance or an EMP event, overall, the U.S. power grid has not been hardened against either.

Question 8. NERC stated that legislation that provided for both standards and other NERC directives to be legally enforceable would significantly enhance cyber security. NERC's alerts process is contained within the NERC Rules of Procedure. Did NERC file these rules with FERC? If yes, what was the stated intent of the alerts program in the NERC filing? Did FERC formally approve these rules? What role, if any, does FERC play in the NERC alerts process?

Answer. Yes, the ERO is required by section 215(f) of the Federal Power Act to file with the Commission for approval any proposed rule or proposed rule change. A proposed rule or change to the rules of the ERO (NERC) may not take effect until the Commission approves the rule. NERC's "alert process" is set forth in section 810 of its Rules of Procedure, "Information Exchange and Issuance of NERC Advisories, Recommendations and Essential Actions." NERC has stated that the purpose of section 810 is to allow NERC to disseminate findings and recommendations from its analyses of major events and information on other events and on potential bulk-power system vulnerabilities. The Commission formally approved section 810 of NERC's Rules of Procedure by order dated February 6, 2008. See North American Electric Reliability Corp., 122 FERC ¶ 61,105 (2008). The Commission's role with respect any NERC advisory, recommendation, or essential action notice is set forth in section 810(5) of the Rules of Procedure. Specifically, NERC is required to give the Commission at least five days prior notice, or less if necessary due to extraordinary circumstances, of NERC's intention to issue an advisory, recommendation or essential action notice This provides the Commission an opportunity to provide input regarding the content of the advisory, recommendation or essential action notice. However, neither the NERC Rules of Procedure nor the Commission's regulations require NERC to accept any Commission input. Further, none of the Alerts are mandatory for the industry to follow.

RESPONSES OF JOSEPH MCCLELLAND TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. Through the definition of "critical electric infrastructure," the discussion draft legislation extends FERC's jurisdiction beyond the Bulk Power System to the distribution level as long as those systems or assets are "vital" to the nation's security, economy, public health or safety. However, as discussed at the May 5th hearing, NERC's authority as the ERO does not extend to the distribution level.

In the discussion draft text, we were trying to respect the Section 215 stakeholder process—the idea being that if FERC directed the ERO to develop or modify a cyber standard to protect "critical electric infrastructure" that standard would be developed through the existing stakeholder process. If FERC found that standard to be inadequate, only then would the Commission be authorized to develop an interim back-stop standard. And that FERC standard would eventually be supplanted by an acceptable NERC produced standard. It was not my intent to allow FERC sole discretion to dictate standards at the local level or bypass the Section 215 process altogether. Please comment.

Answer. I agree that the discussion draft does not eliminate the ERO's standards development role. However, if the ERO fails to submit a timely and adequate standard or modification, the discussion draft would allow the Commission to issue an interim final rule. The discussion draft is unclear on whether the Commission may take such action in other circumstances but, as I stated in my testimony, FERC should be able to require mitigation even before or while NERC and its stakeholders develop a standard, when circumstances require urgent action. Should the Commission require an action on the distribution system, the Commission could rescind the action when no longer necessary. If your intention is to allow the ERO to develop reliability standards to address distribution level cyber vulnerabilities, the discussion draft may need to be modified.

Question 2. The discussion draft defines the term "Critical Electric Infrastructure" as follows:

> . . .means systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce that, as determined by the Commission or the Secretary (as appropriate), are so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety.

To what extent are distribution assets captured in this definition?

Answer. Distribution systems and assets are captured by the proposed Critical Electric Infrastructure definition in the discussion draft, if their incapacity or destruction would have a debilitating impact on national security, national economic security or national public health or safety.

Question 3. Do you read the discussion draft as allowing both FERC and DOE to develop different lists of critical assets? If so, can you provide clarifying language to the Committee?

Answer. Yes. The discussion draft authorizes the Commission or DOE to identify critical electric infrastructure systems and assets. If this approach is deemed inappropriate, the definition of Critical Electric Infrastructure could be clarified as follows:

> The term 'critical electric infrastructure' means systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce that, as determined by the Commission *in consultation with the Secretary* **or the Secretary (as appropriate)**, are so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety.

[Note: For printing purposes, in the above text, italic represents double underlined language and bold represents strike through language.]

Question 4. Currently, how do FERC and DOE work together to assess threats and vulnerabilities? Have there been any problems with this working relationship? How do the two agencies coordinate with the government's intelligence agencies? How does FERC coordinate with NERC on these issues?

Answer. FERC, DOE, DHS, DOD, NRC, FBI, NSA and CIA share information about vulnerabilities to the electric grid. That interaction includes ad hoc meetings on specific topics (such as Stuxnet) and participation in established forums. FERC participates in and supports the Government Coordinating Council for the Energy Sector (for which DOE is the sector-specific agency), the Industrial Control Systems Joint Working Group (organized by DHS) and the Roadmap to Secure Control Systems in the Energy Sector (sponsored by DOE and DHS). FERC also receives technical information and daily reports on threats and vulnerabilities from DHS, the U.S. CERT (Cyber Emergency Response Team), the ICS CERT (Industrial Control Systems CERT) and the SCADA Test Bed. To date, I have not seen any problems with this working relationship.

FERC and NERC coordinate in a number of ways. These include FERC briefing NERC and the industry on threats and vulnerabilities and receiving information through the Electric Sector Information Sharing and Analysis Center (operated by NERC). In addition, FERC works with NERC on every Alert issued to the Electric Sector by NERC. FERC provides technical analysis and input to the Alerts.

Question 5. In your testimony, you note that the Commission has existing authority to direct NERC to develop a reliability standard to address a particular issue, including a cyber security matter, pursuant to Section 215(d)(5) of the Federal Power Act. To date, FERC has not used this authority, which is noted in the DOE/IG report you reference. Why not? Are you aware of any current vulnerabilities that NERC is not addressing?

Answer. The Commission has used its FPA section 215(d)(5) authority to direct the ERO to address cyber security matters. Specifically, on January 18, 2008, in Order No. 706, the Commission directed the ERO, pursuant to section 215(d)(5) of the FPA, to develop significant modifications to the CIP standards the ERO submitted to the Commission for approval to address vulnerabilities identified by the Commission. To date, the majority of the Order No. 706 directed modifications to the CIP standards have not been completed by NERC. Until they are addressed, there are significant gaps in protection such as inadequate identification of critical cyber assets. NERC is in various stages of its standards development process to address these directed modifications. Section 215 of the FPA does not allow the Commission to write or modify the standards, therefore the Commission must rely on the ERO's standards development process to answer the Commission's directives such as those in Order No. 706. This authority is inadequate to address cyber threats and vulnerabilities on the power grid. The DOE-IG report also concluded that this authority was inadequate and recommended the Commission seek additional authority from Congress.

Question 6. You note that the existing reliability standards do not address EMP vulnerabilities. Can't FERC order NERC to produce EMP-related standards pursuant to Section 215? If so, why hasn't the Commission taken such action?

Answer. Yes. The Commission can order the ERO to address EMP vulnerabilities under Section 215. However, to date, the Commission has focused on cyber security issues identified in Order No. 706 which remain largely unaddressed, as explained in question #5 above. In order to better understand the EMP issue and inform our actions, the Commission initiated a joint study with DOE and DHS through the Oak Ridge National Laboratory. This study was just completed September 20, 2010 and was released for peer review at that time. From that time, the Commission has been considering possible options to address this matter including use of its FPA 215 authority. However, the Commission has found the standards development process to be too slow, too open and too undependable to protect the grid from vulnerabilities and threats that can imperil national security. Physical or non-cyber events or attacks, such as an EMP attack, can damage the grid as much as, or more than, cyber attacks. These events might vary significantly and range from natural causes such as solar-magnetic storms to deliberate and coordinated attacks on specific equipment such as bulk power transformers. Legislation including non-cyber vulnerabilities would authorize regulatory requirements, quickly if necessary, to install and actuate protection measures against a solar storm (or threat of an electromagnetic pulse attack) or the stockpiling and sharing of costs for spare transformers.

Question 7. You state that NERC's inclusive stakeholder process, while appropriate for developing routine reliability standards, can serve as an impediment when immediate measures need to be taken to address threats to national security. However, the discussion draft bifurcates federal authority—it tasks DOE with responding to immediate threats and FERC, through the NERC process, with responding to less time-sensitive vulnerabilities. What is FERC's position on this proposed bifurcation? Does the additional authority granted in the discussion draft to the Energy Department for imminent threats address your concerns?

Answer. The discussion draft allows for protection of critical electric infrastructure against all cyber security vulnerabilities and threats. The legislation directs FERC to address cyber security vulnerabilities of the Nation's critical electric infrastructure. These vulnerabilities may sometimes be urgent even if an "imminent danger" of a threat has not yet been adequately documented. To this extent, the discussion draft's authorization for the Department of Energy to address imminent threats is not, by itself, an adequate solution. The discussion draft places the responsibility and authority to address cyber security vulnerabilities of the electric grid with the agency that is already charged with regulating reliability and cyber security of the bulk-power system and is therefore experienced and expert in regulating these matters. Should the discussion draft retain the separation of FERC and DOE responsibilities, FERC expects to coordinate with DOE in order to prevent overlap of our actions regarding FERC's responsibility to address "vulnerabilities" and DOE's responsibility to address "threats." FERC already coordinates with and has an excellent working relationship with many other agencies such as DOE, DHS, DOD, NRC, FBI, NSA and CIA to avoid duplicative or conflicting actions.

Question 8. What is FERC's position on making NERC's Alerts legally enforceable?

Answer. Allowing NERC to issue legally enforceable "Alerts" would vest too much authority in a non-government organization.

Question 9. It appears from your testimony that FERC has been frustrated with NERC's process and timeliness in identifying critical assets. However, NERC's revised "bright-line" proposal for identifying these assets has been pending with the Commission since February. Why hasn't the Commission acted on this proposal to fill in this gap? Couldn't FERC accept this standard and, at the same time, request additional information if needed?

Answer. In February 2011, NERC filed a petition seeking approval of Version 4 of the CIP standards. Version 4 includes new proposed criteria to identify "critical assets" for purposes of the CIP reliability standards. This filing is currently under review by the Commission. Thus, I cannot address its merits at this time. In order to better understand the NERC Version 4 petition, particularly the number of critical cyber assets that will be identified under this revision, the Commission issued data requests to NERC, with responses due on July 11, 2011, which reflects an extension of time requested by NERC. Currently, users, owners and operators essentially have the same discretion as to whether their facilities fall under the CIP standards because there has been no change in method of identifying critical cyber assets in the CIP Standards that are currently in-effect.

Question 10. In the vulnerabilities section of the discussion draft, we have yet to specify the timeframes for FERC's initial determination on the adequacy of reliability standards and for NERC's response to any Commission directive. In FERC's opinion, what is the appropriate amount of time for these actions?

Answer. See the responses to Senator Bingaman's Question Nos. 1 and 2.

Question 11. In the 2007 Energy Independence and Security Act (EISA), Congress directed NIST and FERC to work on interoperability standards for smart grid devices, including cyber security standards. What is the status of this effort? Do the discussion draft's provisions build on or supersede EISA's efforts to improve the cyber security of smart grid devices?

Answer. The most recent Commission action regarding interoperability standards for smart grid devices was a technical conference held on January 31, 2011 to obtain further information to aid the Commission's determination of whether there is "sufficient consensus" that certain smart grid interoperability standards are ready for Commission consideration in a rulemaking proceeding. By notice issued February 16, 2011 the Commission sought industry comments. Comments were filed April 8, 2011 and reply comments were filed April 22, 2011. The discussion draft's provisions complement EISA's efforts to address cyber security of smart grid devices. EISA requires the Director of the National Institute of Standards and Technology (NIST) to coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems. When the Commission finds that NIST's work has led to sufficient consensus, the Commission's task is to institute a rulemaking to adopt such standards and protocols as may be necessary to insure smart grid functionality and interoperability in interstate transmission of electric power, and regional and wholesale electricity markets. Because the smart grid interoperability standards are developed using a consensus approach, similar to NERC's development of reliability standards, the process can be slow. Thus the discussion draft provisions would allow the Commission, if necessary, to move quickly and effectively to address cyber security vulnerabilities that may arise from the implementation of smart grid technology.

Question 12. You testified that you support "clarifications that might better ensure recovery of costs incurred under this legislation." Can the Commission provide proposed text?

Answer. As I stated in my testimony, "it is important that entities be able to recover costs they incur to mitigate vulnerabilities and threats." However, ensuring cost recovery is complex because the affected utilities include not only public utilities regulated under sections 205 and 206 of the Federal Power Act but also nonpublic utilities. Also, some utilities charge cost-based rates while others charge market-based rates. Given these complexities and others, I do not have specific text to suggest at this time, but the affected utilities may have considered this issue in more depth.

Question 13. At the May 5th hearing, you testified that FERC should only get out in front of the ERO in "limited circumstances." Please elaborate. Can FERC provide the Committee with language to capture only these limited circumstances?

Answer. The discussion draft would authorize the Commission to take immediate action to address a cyber security vulnerability, i.e., get out in front of the ERO by issuing an interim final rule, only if the Commission determines immediate action is necessary. The discussion draft language, in subsection (b)(6)(B), appropriately frames these "limited circumstances" as those of immediacy. To clarify this point, however, this subsection could be modified by adding the following at the beginning of subsection (b)(6)(B): "Notwithstanding paragraph (A). . .."

Question 14. The Energy Committee's discussion draft is an electricity-sector only cyber piece. Does FERC prefer a comprehensive, government-wide approach to cyber security issues?

Answer. FERC has no preference, but if a government-wide course is pursued, care should be taken to ensure that the two approaches complement each other, preserving or even enhancing FERC's ability to regulate effectively under legislation such as the discussion draft. The discussion draft would authorize FERC to address cyber security vulnerabilities of the Nation's critical electric infrastructure. By doing so, the legislation places the responsibility and authority to address cyber security vulnerabilities of the electric grid with the agency that is already charged with regulating reliability and cyber security of the bulk-power system and is therefore experienced and expert in theses matters. The discussion draft does not preclude or discourage FERC from working with other agencies or even a central authority (if Congress or the President elects to establish one) to address and mitigate these issues. In fact, in order to be most effective, the Commission would need to coordinate closely with other agencies and bring all resources and expertise to bear on the particular vulnerability or threat presented. FERC already works closely with agencies such as DOE, DOD, DHS, NSA, FBI, NRC, CIA in these matters and expects to continue to do so if the proposed legislation is passed; even in combination with other cyber security legislative efforts affecting other industries and agencies.

RESPONSES OF JOSEPH MCCLELLAND TO QUESTIONS FROM SENATOR UDALL

Question 1. Has the Aurora vulnerability been effectively mitigated, and how is this verified? What is the factual basis for your answer?

Answer. No, I am not aware of any information showing that it has been effectively mitigated. The latest effort to further mitigate the Aurora vulnerability involved NERC and several federal agencies. This mitigation effort included the controlled release to industry of a significant body of technical information about the vulnerability and NERC's issuance of a Level 2 Recommendation in October 2010. The Level 2 Recommendation set forth mitigation steps that asset owners could take voluntarily and required feedback on six related questions. Other than responding to the questions, no actions described in the Recommendation were mandatory. The responses indicated that the majority of the companies had not completed their mitigation plans, their mitigation efforts or even whether the plans would be effective.

Question 2. Are the current spare transformer resources, including the EEI STEP program, sufficient to mitigate the transformer loss scenario presented in the Oak Ridge National Laboratory report from a 1921-level solar storm (over 300 transformers)? What is the factual basis for your answer?

Answer. I do not have any information to substantiate that current spare transformer resources from the EEI STEP program are sufficient to mitigate the projected losses from such a storm—up to 368 transformers.

Moreover, the EEI STEP program was designed as a transformer asset sharing program which assists a participating utility in the restoration of electric service in the event of an act of deliberate destruction of utility substations. This program is designed to reduce the acquisition of transformers by aggregating the needs, in a particular voltage class, among utilities that participate in that program class. While this program may assist any one utility in restoration under a large scale destructive event, it is not designed to mitigate the multiple utility losses as in the case scenario presented in the Oak Ridge Study.

Question 3. How effective has the current standards development process been in protecting against cyber and other non-cyber threats and vulnerabilities to the grid? Is it possible to use this process supplemented with NERC's emergency standards process and the Alerts process to get the job done?

Answer. The current standards development process has not resulted in cyber security standards that adequately protect the grid against cyber vulnerabilities or threats. More than three years has passed since the Commission issued Order No. 706 directing significant modifications to the eight Critical Infrastructure Protection reliability standards. Most of the directed modifications have not been made yet. In addition, the level of sophistication of cyber and other national security threats has increased and more hacker attention is being focused on control systems. NERC's emergency standards process and its "Alerts process" are not enough to bridge the gap in protection. NERC's Alerts are voluntary and are subject to the same limitations as the standards such as open disclosure and unpredictable results. Further, NERC's emergency standards process calls for an urgent action standard to be developed within 60 days and submitted to the Commission for approval or remand (which could be further expedited by a written finding by the NERC board of trustees that an extraordinary and immediate threat exists to bulk-power system reliability or national security). Should the Commission approve the standard, it becomes mandatory for two years and must be replaced, requiring the standards development process to produce a replacement standard. Moreover, while it is untested and unclear, NERC's urgent action procedures could widely publicize both the vulnerability and the proposed solutions before they are even deployed, thereby negating their effectiveness. If faced with a national security risk to reliability, there may be a need for an order by the Commission to act directly; expeditiously, within hours or days, rather than weeks or months; and confidentially, in a manner that protects certain information from public disclosure. Thus, even with NERC's emergency standards process and Alerts process there is a continued need for a process to mandate immediate and confidential security measures. The best method for adopting and implementing mandatory and confidential security measures quickly is through direct federal agency action.

RESPONSES OF JOSEPH MCCLELLAND TO QUESTIONS FROM SENATOR PORTMAN

Question 1. Is it your understanding that the joint discussion draft pertaining to cyber-security of critical electric infrastructure would extend the jurisdiction of the Federal Regulatory Commission to include distribution of assets for purposes of ensuring reliability standards are adequate to protect Critical Electric Infrastructure?

Answer. Yes, see my response to Senator Murkowski's Question No. 2. Distribution systems and assets would be included only if their incapacity or destruction

would "have a debilitating impact on national security, national economic security, or national public health or safety."

Question 2. Since distribution assets are generally under the jurisdiction of the states where they are located, do you anticipate conflicts with various state laws and regulations or, perhaps, other federal initiatives such as interoperability standards for Smart Grid?

Answer. No. The discussion draft would expand the Commission's jurisdiction over certain critical distribution assets for the limited purpose of protecting such assets from cyber vulnerabilities. Thus, this limited expansion of the Commission's jurisdiction would preempt state authority in this discrete area, thereby avoiding any potential conflict. With respect to other federal initiatives, the Commission would coordinate with other agencies, as necessary, to prevent overlap of orders or enforcement actions regarding FERC's responsibility to address cyber vulnerabilities. FERC already coordinates with many other agencies such as DOE, DOD, DHS, NRC, NSA, FBI and CIA to avoid duplicative or conflicting actions.

Question 3. Should conflicts arise, how do you envision these conflicts will be resolved?

Answer. See above response to your Question No. 2.

Question 4. Do you believe that FERC jurisdiction over distribution of assets is necessary?

Answer. Without FERC jurisdiction over distribution assets that fit the definition of critical electric infrastructure, cyber vulnerabilities and threats would not be not be mitigated as proposed by this legislation. Similar to how a compromise at the bulk-power system level could impact the nation, this subset of distribution facilities needs the same level of protection that would be applicable to the bulk-power system to deter against having a debilitating impact on national security, national economic security, or national public health or safety.

Question 5. What do you think will be accomplished that is not already being accomplished?

Answer. With FERC's experience and expertise of the mandatory security requirements to protect the bulk-power system from compromise, FERC can provide an effective protection effort. For example, FERC will be able to address the protection of distribution-level systems and assets, along with their associated physical and virtual connectivity, to protect the reliability or operability of the bulk-power system. This would translate into having the necessary protection measures for certain distribution facilities in concert with measures required for the bulk-power system for national security, national economic security, or national public health or safety.

Question 6. The discussion draft permits FERC to issue an interim rule if the Electric Reliability Organization fails to meet deadlines established by FERC. What do you envision will be the role of the Electric Industry in helping FERC to get an interim rule right?

Answer. FERC's orders and appeals allow the affected industry members to participate whenever practical to help ensure that the measures contained within an interim FERC rule are appropriate for expeditious and effective implementation for security of the bulk-power system. FERC's processes allow the affected utilities the option to engage in the process and provide their perspective and any alternative ideas before they are implemented.

Question 7. Multiple levels of protection on the electric system have significant, additional costs, and may not be the most cost-effective means of mitigating known vulnerabilities or combating known threats. How would you recommend that determinations be made about additional security requirements that are ordered to be put in to place? Should there be a risk assessment required to determine cost-effectiveness?

Answer. The consequences of an entity having an ineffective security posture can be catastrophic, reaching far beyond that entity. Coordinated and simultaneous cyber attacks meant to cause physical damage to large electrical equipment with long lead times for replacement can cause prolonged outages for specific areas of the country. For this reason, considerations regarding cost effectiveness in the cyber security realm are different from the typical cost effectiveness that has been considered for more traditional scenarios. In most scenarios, the limitations and risks are known and quantifiable or at least capable of being estimated based on prior experiences such as severe weather. With cyber security, cost considerations should consider both the known risks as well as ones that have not yet been discovered. In light of these complexities, considerations such as the life-cycle of equipment based on its upgradeability and the consequences of successfully exploiting any cyber vulnerabilities must be considered in addition to more traditional procurement and operational cost measures. For example, according to public reports, the recent Stuxnet malware exploited several zero-day (previously not widely known) software

vulnerabilities. Control system owners were not even aware of these vulnerabilities until months after Stuxnet was launched but their emergence required prompt mitigation regardless of the associated costs. Although this threat was mitigated, cyber security is not a one-time event. It is a continuing process involving technology, security processes and human interaction. Therefore the appropriate showing of cost effectiveness is that the measures taken fit into a comprehensive security program that involves prevention, detection and recovery from a security breach.

RESPONSES OF JOSEPH MCCLELLAND TO QUESTIONS FROM SENATOR SHAHEEN

Question 1. I've heard from the NH electric co-operative about their concerns in granting FERC authority to regulate at the distribution level of our electric system. Regulation at this level is traditionally handled by the state. What authority, if any, does FERC have right now to regulate distribution facilities in the U.S.?

Answer. Section 215 of the Federal Power Act expressly does not apply to local distribution facilities. These facilities are also generally exempt from FERC's rate regulation, although limited exceptions apply if the facilities are used in providing FERC-jurisdictional services. The additional authority over distribution facilities proposed in the discussion draft would be very limited in nature. It would only allow the Commission to regulate distribution facilities that are "so vital to the United States that the incapacity or destruction of the systems and as sets would have a debilitating impact on national security, national economic security, or national public health or safety." In addition, the current proposal would only allow the Commission to regulate that discrete set of facilities for the purpose of addressing cyber security vulnerabilities.

Question 2. The current NERC standard development process is a "bottoms up" approach that works with electricity sector experts in the U.S. and Canada to develop technical standards that take into account the different among more than 3000 individual North American utilities. Why does FERC think this should be replaced with a standards process that would emanate from Washington, DC?

Answer. FERC does not think that the current NERC standards development process should be replaced. And the discussion draft does not eliminate or replace the NERC standards development role. The standards development process will continue to be performed by the ERO and industry unless there is a need for immediate action. The discussion draft would only allow the Commission in very limited defined circumstances to directly, quickly and confidentially address cyber security vulnerabilities that threaten national security through the power grid.

RESPONSES OF WILLIAM TEDESCHI TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. Your testimony states that it may be possible to mitigate electromagnetic threats to the power grid through selective hardening. Could you describe some of the ways in which utilities could selectively harden their systems?

Answer. The utilities have available two primary opportunities for selectively hardening the power grid. (1) They can wait until new technologies or planned system upgrades are to be introduced to the grid, and then apply some form of EMP hardening requirements that can be incorporated in the acquisition process for those new/upgraded features to be procured and introduced to the grid. (2) The other major possibility is that they can choose to retroactively harden key elements of the current grid, by procuring electronics hardware with specifically designed hardening features incorporated into the hardware design. The former approach is recommended, as adding hardening after a system has been fielded is typically more expensive. However, if a particular grid element or node is critically important and susceptible to EMP threats, then one may wish to retroactively add hardening to the existing design and make it more robust to EMP threats.

There are specific hardening approaches that can be selectively employed at the hardware, box, and device levels. The principle that applies is to define, anticipate, and plan to harden against select EMP threat environments. For highfrequency EMP threats, such as unintentional electromagnetic interference or malevolent microwave devices, in the many megahertz to gigahertz frequency range, one can require new electronics have existing electromagnetic compatibility and interference (EMC/EMI) standards incorporated into their design. Such standards are published by both national and international organizations, based on subject matter expert inputs and endorsed by industry, governments, and academia. Hardening features can include the following: properly shielded and grounded enclosures; fast-acting overcurrent shunts or blocks at points of entry; spark gaps and other over-voltage protection; better internal design robustness against over-current and over-voltage conditions, and direct-current or slowly varying offsets (such as better design features

inside highvoltage transformers); and electronic filters that are highly selective in the frequencies of electronic transmissions around and into critical grid elements or nodes with operating electronics inside. Hardening can also include creating a more-robust control system for real-time and near real time monitoring and adjusting the actual operation of power flow into, over, and out of the grid, to effectively sense, understand, and respond to a greater range of off-normal conditions during grid operation. Many of these same hardening approaches, and other related techniques not mentioned, can also be considered for the low-and medium-frequency EMP threats, in the many hertz to megahertz frequency range. The type of hardening one might consider employing and at what point in the grid's life cycle should be based on a good understanding of the EMP threat spectrum, what hardware, device, or electronics box is susceptible to EMP attack, and the identified trade-offs in cost, benefit, and risk reduction for the various types of possible hardening approaches.

Question 2. Your testimony states that more work is required before fully informed decisions can be made about where and to what extent the grid should be hardened solely against nuclear electromagnetic pulse threats. What kind of information would additional work on electromagnetic pulse threats seek to produce? How long would you estimate that this study may take?

Answer. The additional information we recommend to be generated is to determine an appropriate set of EMP threat scenarios that could adversely affect the power grid, determine if and how the grid is susceptible/vulnerable to the established EMP threats, and identify appropriate threat mitigation and hardening strategies. This set of work (see next paragraph for details) is estimated to require from 2 to 3 years to accomplish, depending on the number of EMP threat classes selected and the amount of technical resolution in the results required to reduce existing uncertainties to an acceptable level and provide a level of riskbased confidence in the current and projected resilience of the power grid.

The full spectrum of possible nuclear high-altitude EMP threats should be examined and characterized, beyond what has been considered to date, namely, only the postulated worst-case nuclear EMP threats. The resulting over-current and over-voltage insults to the grid will be of lesser magnitude and total energy content than the worst-case assumptions that have been made to date, but the worst-case system response may not always be driven by the largest magnitude EMP conditions. The spectrum of possible conventional EMP threats, both malevolent and unintentional, should also be examined and characterized. In particular, what are the technical characteristics of all the postulated EMP threats in terms of their waveforms, frequency content, and electric field strengths? These EMP threat waveforms, along with those postulated from solar-induced geomagnetic storms, should be peer reviewed and validated by a panel of knowledgeable subject matter experts. Next, these EMP threat waveforms can be projected onto selected key elements of the U.S. power grid, and the induced over-current/over-voltage insult estimated by using a combination of computerbased modeling and simulation, along with experimental testing. Threatened key elements of the grid, given a particular EMP threat scenario, can be identified from our knowledge of the grid's network topology and unique design features. Once the electrical insults for the key grid elements are determined, one would ascertain if the element is susceptible to upset or burnout, or other possible adverse effects. Thresholds for upset and burnout would be determined through a combination of computational and experimental modeling and simulation, and by using a somewhat different set of tools and subject matter experts. Given a projected set of upset and/or burnout conditions, one would finally estimate the net cumulative effect (or consequence) on the power grid given the particular EMP threat waveform that was projected against a particular set of grid elements. Once the complete set of risks to the power grid is characterized and better understood—given the full spectrum of possible EMP threats and resultant possible damage responses and ultimately consequences to the grid's continued operability—one can make more informed decisions on whether, where, and to what extent to harden the grid against certain classes of EMP threats. All the work results should be peer reviewed and validated by appropriate subject matter experts, and relevant work conducted in the past should be utilized to the maximum extent possible.

Responses of William Tedeschi to Questions From Senator Murkowski

Question 1. Your testimony notes that more study is needed to characterize and simulate the susceptibility of the power grid to EMP attacks, and that existing EMP reports should not be the basis for any short-term national decisions. Is it premature to develop hardening standards to mitigate an EMP attack?

Answer. Yes, today it is premature to develop hardening standards for the power grid against EMP threats, both malevolent and non-malevolent (i.e., unintentional

and naturally occurring geomagnetic threats). The spectrum of possible EMP threats has not been defined and characterized, and neither has the susceptibility of key grid elements to EMP-induced over-current/over-voltage insults, along with the possible resultant damage and consequences to the continued reliable operation of the grid. For example, the 2010 FERC-sponsored study on EMP threats to the power grid suggests that over 300 high-voltage (HV) transformers would be at risk for damage or failure by a 1-in-100 year geomagnetic storm. This damage estimate appears to have been based primarily on one data point, an estimated 90-amp over-current insult to an HV transformer that failed at the Salem Nuclear Plant during the 1989 geomagnetic storm. Applying that particular over-current damage threshold, based on little analysis and no experimental testing, to all HV transformers in a large-area geomagnetic storm results in great uncertainty about the total number of at-risk HV transformers. We assess that this is a worst-case approach to predicting when HV transformers could fail due to over-current insults. The Salem Nuclear Plant HV transformer could have failed for a number of reasons. We recommend that the specific reasons for that failure, as well as consideration of the suite of other possible failure thresholds and conditions, should be better understood so that, ultimately, a more-balanced damage criteria can be established, which will result in a better estimate of the potential damage and consequences to the grid, not only from geomagnetic EMP threats, but also from other EMP threats. We recommend more analysis, experimentation, and assessment be performed to determine how and why HV transformers can fail, along with other key elements of the grid. There simply is not enough data and understanding at this time on how and why key power grid elements can fail to the spectrum of possible EMP threats. Once the additional data and understanding are derived, a defensible technical basis exists for developing and implementing a national hardening strategy.

Question 2. Do parts of the power grid, and particularly transformers, based on age and design, react differently to an EMP attack? Do we need to treat all of them in the same manner?

Answer. Yes, every element in the power grid when exposed to EMP attack will react differently to the over-current/over-voltage insult caused by the EMP attack. How each grid element will react depends on a number of factors: the element's design, as-manufactured configuration, current configuration if it has been changed or modified, age and location within the grid topology; installation details; how the EMP threat irradiates and couples electrical energy into the exposed element; how that electrical energy insult flows within the element and deposits its energy along the way; and the strength of the element to withstand the flowing and deposited electrical energy. The full range of possible outcomes of the exposed grid element to the EMP attack include temporary damage or upset, permanent damage, and possibly even no damage or adverse effect. One must also factor in the interplay of how one element's response to the EMP attack will affect the operation of other elements that are connected to it. As far as treating each element in the same manner, one must demonstrate a sufficient understanding of the differences between each element of the grid, and how they will respond to the EMP insult both in their own unique way and synergistically together, if one is to have confidence in estimates of how an EMP attack might affect the grid. EMP effects researchers use analysis, modeling, and experimental testing to conduct detailed characterizations of the design and key operational functioning aspects of all the elements making up a network and of how the element (and ultimately the grid) will react to the deposited electrical energy from the EMP attack. Even within a population of similar grid elements, for example 300 HV transformers, there are enough differences in the design and constituent materials that go into the element and how the element was manufactured that the element's response to the EMP insult can vary by more than an order of magnitude, and sometimes the failure distribution follows well-established statistical distributions; at other times, it does not. The result is that for the same EMP attack, anywhere from a small fraction (or none) to a large percentage of the element's population can be adversely affected. The predicted damage depends very heavily on when and how the transformer (or element) might fail, and more than one data point and significant analysis and modeling are required to get a level of confidence in the expected damage prediction. It is this analytical and experimental modeling and simulation phase of characterizing the grid element and interconnected network that takes a while and a certain amount of resources to establish a level of understanding and confidence in the result. In the absence of data and understanding, and given limited time and resources, researchers typically employ a worst-case approach that unfortunately can lead to a higher cost impact and dire predictions that are not technically defensible, and should not be the basis for important national decisions of this type.

Question 3. You mentioned that the U.S. electric power grid contains some level of inherent hardness against an EMP impact, and that the grid is already somewhat hardened against the E2 and E3 components (similar to lightning strikes (E2) and solarinduced geomagnetic storms (E3)). However, since the E1 frequency strikes first, how vulnerable is the grid to the E2 and E3 impacts if it has been disabled by the E1 component? Should our focus be on the E1 frequency? Or should it be on the E3 component since you believe a solar-induced geomagnetic storm is more likely than a nuclear-induced EMP attack?

Answer. Yes, for nuclear-detonation-generated EMP, the early-time E1 component, if strong enough, could do damage first to some grid elements or control systems, potentially resulting in the later-in-time E2 and E3 components doing additional damage to the grid. In other cases, the E1 component may not be strong enough to do any damage, but the E2 and E3 components will insult the grid, potentially doing damage. Again, details of the nuclear detonation will affect the extent and strength of the EMP effects and are relevant to whether damage might occur. In some nuclear scenarios, none of the E1, E2, and E3 components would be expected to do damage on the power grid. In general, the E3-like component that results from geomagnetic storms occurs naturally and with an established periodicity. It is just a question of when the storm will occur, how strong it may be, and how long the created electromagnetic field strengths would last, and then whether the power grid is susceptible to them and what might be the possible damage effects. The nuclear E1, E2, and E3 components are human-made, and are assessed to be of low likelihood of occurrence, as compared with geomagnetic storms and some of the electromagnetic interference threats. We should also consider human-made malevolent EMP-generating devices, which can be used to exacerbate a particular frequency range, or multiple ranges. You are exactly right: The combination of imposed reduction of capability from one frequency range and imposition of a different frequency range is another topical area that should be included in studies of system response.

Question 4. What different types of protection are needed and available for the various types of potential EMP attacks or geomagnetic disturbances?

Answer. As noted above in the answer to Senator Bingaman's first question, there are many hardening approaches, both passive and active that could be considered and applied to the power grid that would add an elevated level of resilience against EMP threats. Once the EMP threats have been sufficiently characterized and an assessment made with at least a moderate level of confidence of the grid's susceptibility and resultant damage to such threats, then costeffective risk-based decisions can be made regarding a national hardening strategy and specific hardening measures to employ. Our recommended approach is to characterize the full spectrum of EMP threats, both intentional (nuclear and nonnuclear) and unintentional (electromagnetic interference) human-made and naturally occurring (geomagnetic). Next, we should more fully characterize the grid's susceptibility to potential damage by those classes of EMP threats (through analytical and experimental modeling and simulation), and identify possible techniques to harden against the identified threats. At a minimum, we should ensure that we are hard against unintentional human-made interference (which is a threat now) and have an acceptable level of resilience against geomagnetic EMP threats (which is a work in progress). Next, we should establish how resilient or susceptible/vulnerable the grid is to the human-made EMP threats, and then finally make risk-based national and/or industry-level decisions on whether and to what extent to harden certain elements of the power grid against the broader set of EMP threats. That said, risk-based analysis and assessment approaches should continue to be applied looking for key grid elements and nodes that might be vulnerable to specific EMP threats and which might need to be hardened sooner rather than later.

Question 5. Are smart grid technologies that are currently being distributed across the country and placed into service required to have hardened features to protect against EMP attacks?

Answer. Our understanding is that smart grid technologies that are currently being considered and possibly distributed across the country and placed into service are not required to have hardening features to protect against EMP attacks. The smart grid technologies at a minimum should have a level of hardening against lightning and unintentional electromagnetic interference (EMI) based on some combination of national and international EMI and electromagnetic compatibility (EMC) standards. If EMI and EMC standards are being considered and included in new smart-grid technologies, then they will have some level of resilience against E1-type EMP effects. How much resilience there is or might be can be determined through a combination of analytical and experimental modeling and simulation. Because possible smart-grid technologies are still under development, are generally small and

likely will be mass-produced and therefore lower in per unit cost than, for example, HV transformers, there is an excellent opportunity here to consider and possibly include some form of costeffective, EMP hardening features to protect against E1-and E2-like EMP threats.

RESPONSES OF PATRICIA HOFFMAN TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. Last year, Secretary Chu announced funding for the National Electric Sector Cyber Security Organization. What is the role of this organization vis-a-vis North American Electric Reliability Corporation (NERC), NERC's standards development process, and the Federal Energy Regulatory Commission?

Answer. The Energy and Water Development Appropriations and Related Agencies Appropriations Act, 2010 (P.L. 11-85) directed that "...the Secretary shall establish an independent national energy sector cyber security organization..." In response, the Department of Energy issued a Funding Opportunity Announcement on March 31, 2010. Two organizations received awards: EnergySec was selected to form the National Electric Sector Cybersecurity Organization (NESCO). The Electric Power Research Institute (EPRI) was selected as a research and analysis resource to this organization, and is referred to as the National Electric Sector Cybersecurity Organization Resource (NESCOR).

The purpose of the award was to "establish a National Electric Sector Cyber Security Organization that has the knowledge, capabilities, and experience to protect the electric grid and enhance integration of smart grid technologies that are adequately protected against cyber attacks." In addition, the organization "will serve as a focal point to bring together domestic and international experts, developers, and users who will assess and test the security of novel technology, architectures, and applications." When fully operational, NESCO/NESCOR will provide early warnings to and share best practices with, all parts of the sector (generation, transmission, distribution), not just the bulk power system. NESCO/NESCOR will provide comments to the North American Electric Reliability Organization (NERC) standards development process as appropriate and share compliance information in the sector, but does not enforce or regulate the standards.

NERC's mission is to ensure the reliability of the North American bulk power system. NERC is the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission (FERC) to establish and enforce reliability standards for the bulk-power system. NERC develops and enforces (following approval by FERC) reliability standards, including cyber security standards; monitors the bulk power system; and educates, trains and certifies industry personnel. NERC is an authoritative body and can mandate actions by the registered entities. NESCO/NESCOR is a voluntary body that can provide guidance.

Question 2. In February, the Department of Energy launched an open collaboration with the National Institute of Standards and Technology and the North American Electric Reliability Corporation to "develop a cyber security risk management process guideline for the electric sector." Could you describe the objectives of this collaboration and how its work will filter into the NERC standards development and approval processes?

Answer. DOE, in coordination with the National Institute for Standards and Technology (NIST) and NERC, is leading a public and private sector collaboration to develop a risk management process guideline to provide a consistent, repeatable, and adaptable process for the electric sector, and enable organizations to proactively manage cyber security risk. The objective of this collaboration is to build upon existing guidance and requirements to develop a flexible risk management process tuned to the diverse missions, equipment, and business needs of the electric sector for application throughout the sector, and to bridge the divide between security for industrial control systems and information technology. The risk management process guideline is currently in the drafting stage. Representatives from the NERC standards development team are participating in drafting of the risk management guideline. As this effort gets further along we will better be able to assess how it may factor into the NERC standards development and approval processes.

Question 3. Your testimony states that the Department of Energy and the Department of Defense have signed a memorandum of understanding that is intended to enhance national energy security. The Discussion Draft directs the Secretary of Defense to prepare a plan to protect power supplies to national defense facilities. How will this memorandum help the Secretary of Defense in creating this plan?

Answer. The Department of Energy and the Department of Defense (DOD) energy security Memorandum of Understanding (MOU) provides for collaboration between the two agencies on energy security research and development, and energy assur-

ance. This may include projects on power electronics, microgrids, cyber security, electromagnetic pulse, smart grid, and storage which will benefit from DOE's energy related expertise. An Executive Committee has been formed to oversee all activities, including energy security. The Executive Committee is chaired by me, as the Assistant Secretary for Electricity Delivery and Energy Reliability, DOD's Assistant Secretary of Defense for Operational Energy Plans and Programs, and DOD's Deputy Under Secretary of Defense for Installations and Environment. The remainder of the Executive Committee is comprised of key energy decision makers from both departments.

While this MOU is not focused on cyber security for the grid, it provides a structure to collaborate on a comprehensive proactive 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.

Question 4. Do you think each state has adequate cyber expertise to protect distribution-level systems and assets that are so vital that their loss would have a debilitating impact on national security, national economic security, or national public health or safety?

Answer. Local distribution companies, and the Public Utility Commissions (PUCs) that regulate them, are the entities at the State level that are responsible for reliable electric service within states, including protection from service disruptions caused by cyber attacks. It is DOE's understanding that the utilities and PUCs understand, and are addressing cyber security concerns. States, similar to the Federal government and the private sector, are challenged by the increasing sophistication of the threat to maintain a level of cyber security expertise adequate to manage cyber security risks.

State and local governments are very concerned about the impacts of cyber attacks and are taking steps to address such risks. The Department also recognizes the need to mature and increase the level of cyber security expertise within the states and the electric sector. The Department's Office of Electric Delivery and Energy Reliability (OE) works closely with organizations, such as the National Association of Regulatory Utility Commissioners (NARUC), the National Association of State Energy Officials, the National Conference of State Legislatures, the National Governor's Association, and Public Technology Institute that are helping State and local agencies to address cyber security issues. These organizations have worked with OE to develop technical briefs, education forums, workshops, and exercises on cyber security and other concerns related to grid modernization. OE has been working with these organizations to support and sponsor activities such as the NARUC security boot camp provided for PUCs and their staff at the 2011 NARUC winter meeting, and providing technical assistance to PUCs related to cyber security for the smart grid.

Through the American Recovery and Reinvestment Act, OE provided funds to forty-eight states and territories plus forty-three cities to prepare energy assurance plans to better respond to energy emergencies, including addressing cyber security. States have recently completed draft emergency assurance plans all of which address cyber security. Recovery Act funds are also assisting state public utility commissions directly, providing funds to hire new staff and retrain existing employees to ensure they have the capacity to quickly and effectively review proposed electricity projects, including the cyber security aspects of those projects.

RESPONSES OF PATRICIA HOFFMAN TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. Currently, how do DOE and FERC work together to assess threats and vulnerabilities? Have there been any problems with this working relationship? How do the two agencies coordinate with the government's intelligence agencies?

Answer. DOE and the Federal Energy Regulatory Commission (FERC) coordinate on an ongoing basis depending upon the specific nature of the critical infrastructure protection activity. Most recently, DOE, FERC, and the Department of Homeland Security (DHS) sponsored a set of reports[1] which provided a technical threat assessment of geomagnetic disturbances and electromagnetic pulse, providing a more comprehensive understanding of the issues. FERC is also participating in the effort led by DOE, along with the National Institute of Standards and Technology (KIST), DHS, and North American Reliability Corporation (NERC), to develop a risk management process for the electricity sector specifically aimed at providing the sector with a common and repeatable cyber security risk management process.

[1] Prepared by Metatech Corporation under the direction of Oak Ridge National Laboratory. Available at http://www.orni.govisci/ees/etsd/pes/ferc__ernp__gic.shtml

Threats to the electricity sector are an operational issue and thus should principally be handled by DOE as the Sector Specific Agency (SSA) under Homeland Security Presidential Directive 7 and the National Infrastructure Protection Plan (NIPP). Effectively responding to potential threats to the sector requires an operationally-oriented organization with established coordination mechanisms with DHS and the intelligence community to properly assess and respond to a threat. DOE is able to draw from a variety of resources, including its Office of Intelligence and the resources of the National Laboratories to effectively assess and respond to emerging threats to the sector. This is all done in close coordination and collaboration with DHS, FERC, and other Federal partners under the National Cyber Incident Response Plan and most importantly, in coordination with the electricity sector.

To be effective in its roles as the SSA, DOE depends upon and constantly works to build and strengthen its relationships with utilities and the broader electricity sector stakeholder community. DOE fosters collaboration and voluntary initiatives to further its goal of a reliable and resilient power grid. Given FERC's role as an independent regulator, DOE has found that discussions with industry can sometimes be more open and frank if FERC is not present. This is consistent with the philosophy of the NIPP which sought to facilitate open and candid conversations on infrastructure security issues under the public-private partnership.

Question 2. The Energy Committee's discussion draft is an electricity-sector only cyber piece. Does the Department prefer a comprehensive, government-wide approach to cyber security issues?

Answer. Yes, recognizing the interdependencies between different sectors it is important to have a comprehensive, government-wide approach to cyber security. The Administration has proposed comprehensive cyber security legislation (http://www.whitehouse.gov/ombilegislative_letters).

Question 3. Recently, Howard Schmidt, the White House cyber security coordinator, made headlines when he said that the risks of cyber attacks is often overblown and that cyber attacks are the "risk of doing business." In light of these statements, does the Administration believe additional Federal authority is needed in the cyber security arena?

Answer. We often associate high profile events with the term "cyber attack," but the reality is our networks face a spectrum of risks, many of which are less spectacular yet more pervasive. Our federal networks, as well as many of those that support our critical infrastructure are probed thousands of times per day. Managing and responding to these risks has become a core element of how we as a nation do business, and an important aspect of ensuring the reliability of the grid. Cyber security standards can provide an effective baseline to address known vulnerabilities.

Managing the risk from unknown vulnerabilities and dynamic threats are best addressed by timely sharing of relevant and actionable threat information, the use of risk management, and effective incident management and response. The electricity sector must have the ability to assess, respond, and mitigate the impacts of an event in a timely manner.

Question 4. I understand that DOE is working on the need for domestic manufacturing of transformers. Please elaborate on the problem and what is being done on this issue.

Answer. The U.S. is heavily dependent on imports for large transformers above 345kV. In addition, limited manufacturing capacity results in long lead times for delivery of high voltage transformers, often over 12 months. This situation is of concern to the Department.

Import dependency is of concern to the utility industry, as well as DHS/FEMA and DOD. DOE has held discussions with several transformer manufacturers, including ABB, Efacec, Waukesha and Areva, and additional discussions are planned. The DOE-North American Electric Reliability Corporation (NERC) workshop report on High-Impact, Low-Frequency Event Risk to the North American Bulk Power System (June 2009) identified this as an important concern. Large transformer concerns were also identified in both the 2007 and 2010 Energy Sector Specific Plans. Even with the successful start up of new manufacturing facilities, only a small portion of U.S. utility annual demand is likely to be rnet. Additionally, a significant national level disaster impacting a large number of transformers would certainly exceed domestic manufacturing capability and would likely require the global market to significantly ramp up production to meet the demand.

In 2009 a new plant was opened in Georgia by Efacec and two other companies (Mitsubishi and Hyundai) have announced new plants to be built in the U.S. A domestic manufacturer Waukesha Electric Systems has begun to expand their production capacity to 500kV and 765kV units in their Waukesha Wisconsin facility. DOE has also partnered with the Department of Homeland Security to develop and test

a lighter weight and more transportable, temporary transformer that could be used in emergencies.

Question 5. What is the Administration's position on the bifurcation of federal authority set forth in the discussion draft? Do you believe FERC needs additional authority to address vulnerabilities or is the existing Section 215 stakeholder process adequate?

Answer. The Administration does not have a position on this particular discussion draft, but has proposed comprehensive cyber security legislation (http://vvww.whitehouse.gov/ombilegislative_letters).

With respect to emergency authority, when the Department of Energy and FERC were established by the Department of Energy Organization Act, the Secretary was given the authority to issue orders during an emergency for the interconnection of facilities, generation, delivery, interchange, or transmission of electric energy. FERC was given Federal Power Act (FPA) authority to establish, review and enforce rates and charges for the transmission and sale of electricity. DOE believes that these divisions of FPA authority properly place the regulatory rate making responsibilities of the FPA with FERC, and the authority to make national emergency determinations with DOE.

We believe that emergency authority is appropriately placed with the head of a cabinet department who is fully accountable to the President. DOE and DHS have the capability to develop or obtain knowledge with respect to threats or vulnerabilities that might give rise to the need for an emergency order.

Question 6. Do you agree with Mr. Tedeschi from Sandia National Laboratory that the susceptibility of the power grid to EMP attacks is not well characterized and should be further addressed with computer-based simulations and experimental testing?

Answer. Yes, we absolutely agree with the concerns raised in Dr. Tedeschi's testimony. As he noted "Assumptions about age, design, and failure thresholds of transformers introduce additional uncertainty and are based on limited samplings of transformers of a particular type and from a clear source. All assumptions point to large uncertainties in the output results and interpretations from the model; therefore, statements on the number of 'at-risk' transformers and the severity of the regional damage should be viewed as illustrative only."

Computer-based simulations are needed to support electric utility adoption of technological approaches to reduce the threat of electro-magnetic pulse (EMP) attacks and solar storms. These will assist utilities to develop an understanding of the potential impact of EMP on the power grid and its components. Utilities run computer simulations to help optimize power production and transmission and to avoid failures. Ultimately, technological solutions will require research and development and careful testing and evaluation to ensure their effectiveness.

Responses of Patricia Hoffman to Questions From Senator Udall

Question 1. Has the Aurora vulnerability been effectively mitigated, and how is this verified? What is the factual basis for your answer?

Answer. The Aurora vulnerability has been effectively studied and analyzed. The fundamental principles behind the Aurora vulnerability are well understood by experienced and practicing utility engineers and operators. Assessment of the effectiveness of the mitigations is currently underway.

In early 2011, the ES-ISAC issued an Essential Action Advisory to all NERC registered entities to provide the additional technical details that described the nature of the vulnerability and assess the current status of mitigating actions implemented by registered entities through this action. NERC will also use the information to determine what additional actions may need to be taken. The Department anticipates the Aurora vulnerability will be addressed by NERC entities and verified.

In 2007, DHS, DOE, other Federal agencies, and NERC' s Electric Sector Information Sharing and Analysis Center (ES-ISAC) became aware the Aurora vulnerability which, if exploited by an attack, could cause significant physical damage. The ES-ISAC issued an advisory to describe the mitigation measures that electric sector owners and operators needed to implement to reduce the risks associated with the Aurora vulnerability. Unfortunately at that time, the supporting technical documents could not be released to the owners and operators due to the documents' classification level.

The Department has supported NERC and the sector through the development of the 2011 Essential Action Advisory and its accompanying documents. The Department continues to support Department of Defense efforts to mitigate the Aurora vulnerability and protect its military installations.

Question 2. Are the current spare transformer resources, including the EEI STEP program, sufficient to mitigate the transformer loss scenario presented in the Oak Ridge National Laboratory report from a 1921-level solar storm (over 300 transformers)? What is the factual basis for your answer?

Answer. The EEI STEP program is focused on sharing of spare transformers to assist recovery from a terrorist attack. EEI reports that some 50 utilities representing approximately 70 percent of the electricity customers are participating in this program. The vast majority of smaller utilities including municipals and coops are not participating.

The adequacy of existing spares to address major transformer outages will depend on many factors including the geographic impact, the type of transformers, the age and health of the transformers. But, it is clear that major transformer losses from a solar storm of historic magnitude would present an enormous challenge to the sector's ability to respond to and recover from such an event. The North American Electric Reliability Corporation (NERC) is addressing the spare transformer issue and has created a Spare Equipment Database Task Force, as well as, a Task Force on Geomagnetic Disturbances. NERC will seek information from all of its member companies. Several transformer manufacturers including ABB and Siemens are participating on the NERC task forces as well.

There are limited modeling studies to provide a factual basis to estimate possible electricity grid impacts to a 1921 magnitude solar storm. Utilities in Canada, the United States and Europe have begun to take steps to reduce the potential impact of such large solar storms. The North American Electric Reliability Cooperation has recently issued an alert to its members on steps that they may take to reduce potential impacts on their equipment and the grid. [See: http://www.nerc.com/fileUploads/File/Events%20Analysis/A-2011-05-10- 01__GMD__F1NAL.pdf]. The alert was the result of a 2-day NERC workshop in April 2011 to discuss utility approaches to address the issue. DOE is working with electricity industry partners to increase attention and to encourage the use of best practices.

Question 3. How effective has the current standards development process been in protecting against cyber and other non-cyber threats and vulnerabilities to the grid? Is it possible to use this process supplemented with NERC's emergency standards process and the Alerts process to get the job done?

Answer. What is most important is that a structure exists to support an "electric sector incident response plan" to respond to events. A combination of the NERC standards and Alerts process, timely and actionable information sharing, and emergency authority will provide a comprehensive approach to managing cyber security threats and vulnerabilities. Standards ensure a level of quality, compatibility, safety, and connectivity with other equipment and processes.

Standards must be widely accepted and commonly trusted to be effective. They also provide the foundation for further innovation, or as in the case of security or safety, a minimum level of requirements. As a result, standards development is often a time-consuming process. Development of security standards relies on awareness and consensus of the threat environment. This is a challenge to the electric sector due to the dynamic nature and speed of cyber threats that necessitates access to timely and actionable threat information. This challenge makes it difficult to adequately assess impact to inform risk decisions on investment in cyber security improvements beyond what is needed for compliance.

Responses of Patricia Hoffman to Questions From Senator Portman

Question 1. It is my understanding that the discussion draft grants the Secretary of Energy the authority to require others to take actions if 'the Secretary determines that immediate action is necessary to protect critical electric infrastructure from a cyber security threat." The Secretary may then follow a procedure to make these requirements permanent. In your opinion, what sort of event would trigger such an action by the Secretary?

Answer. The discussion draft grants the Secretary of Energy the authority to require others to take actions if the Secretary determines that immediate action is necessary to protect critical electric infrastructure from a cyber security threat." The type of event that would trigger such action by the Secretary would be an event that poses a significant risk to the operation of critical electric infrastructure, such as high altitude electromagnetic pulse, or a cyber attack. The determination of whether to use emergency authority would be based on analysis of the threat, evaluation of risk and consequences, and the potential for impact to electric sector and potential other sectors of the economy. Additionally, use emergency authority would be determined in consultation with other sector specific agencies that could be potentially impacted.

Question 2. Why would the Secretary make a requirement permanent?

Answer. It is DOE's understanding of the discussion draft that cyber security mitigation actions required by an emergency order would not be permanent, but limited to 90 days unless renewed. However, where appropriate these actions could be incorporated through the accelerated standards or NERC Alerts process.

Question 3. Multiple levels of protection on the electric system have significant, additional costs, and may not be the most cost-effective means of mitigating known vulnerabilities or combating known threats. How would you recommend that determinations be made about additional security requirements that are ordered to be put in to place? Should there be a risk assessment required to determine cost-effectiveness?

Answer. Risk assessments should be used to determine cost effectiveness of security requirements. The NERC-CIP security requirements were developed through an industry-led collaborative effort that considered risk assessments and the cost-effectiveness of these requirements. Additionally, the NIST "Cyber Security Guidelines for the Smart Grid" NISTIR 7628 provides guidance on defense-indepth strategies and risk assessments. Federal (FERC) and State regulators should consider cost and assessment of risk, including impact, when determining additional security requirements.

RESPONSES OF PATRICIA HOFFMAN TO QUESTIONS FROM SENATOR SHAHEEN

Question 1. As the witnesses have noted, the electrical grid is a very tempting target for cyber attacks in the United States. According to the U.S. Computer Emergency Readiness Team, cyber security incidents involving government computers have gone up by a factor of 10 in the past five years. Are electrical utilities and the grid seeing the same sort of rapid growth in the cyber security threat to their facilities?

Answer. In general, the utilities like government agencies face thousands of scans and probes every week. For example, during periods of heightened awareness, a large utility may have to analyze millions of log entries in a day to ensure that their defenses have not been breached. The spectrum of cyber security incidents ranges from reconnaissance-type scans and probes of corporate networks to an attack such as Stuxnet that reaches into more isolated control systems networks.

The number of cyber security incidents is not necessarily an indication of intent or likelihood of a significant attack. The Department, DHS, NERC, and FERC all receive different levels of specificity in reporting on cyber incidents based upon their different responsibilities. In addition, larger utilities have security operations center that monitor and track cyber incidents. For example, DOE funded an effort to develop a cyber security operations center for a major utility. This effort has been successful in bringing together trusted entities outside of the utility's region to share information about cyber incidents. The lesson learned is the large investment in time, resources, and relationship-building is necessary to develop enough trust to share the information.

In addition to building trust, consistently defining cyber security incidents and sharing threat information between utilities is a challenge. Currently, there is no collective, consensus-based cyber threat assessment. DOE works with several entities to determine and assess the cyber security threats to the sector. Internal DOE resources provide expertise and information including the Office of the Chief Information Officer which provides cyber security expertise and threat information; the Office of Intelligence which provides early warnings and indicators, and intelligence reports directly related to the energy sector; and the National Laboratories which provide both cyber security expertise and threat information. DOE also partners with NESCO/NESCOR, DHS, NERC, the intelligence community, law enforcement, electric utilities, and cyber security consultants to determine and assess the threats, and share that information with the sector.

Question 2. Given that we haven't had a major disruption of electrical service due to a cyber attack, does this mean the current standards process is working?

Answer. Standards are effective in providing baseline levels of performance, but standards alone are not effective in facilitating or encouraging an adaptable and agile cyber security organization. They can also lock organizations into making cyber security decisions that may not be optimal for their system in order to comply with the prescriptive nature of a standard. The standards development process under section 215, because of its need to reflect multiple stakeholders with different cyber security issues and concerns, is an inherently slow process and thus will never be able to fully counter the threats posed to the sector. In this dynamic threat environment, new threats emerge without warning utilizing new attack vectors. Thus, organizations must be vigilant and adaptable in monitoring their systems and im-

plementing proper controls in response to current threats. A standard cannot achieve this outcome. A combination of NERC standards and Alerts process, timely and actionable information sharing, and DOE emergency authority would provide a more comprehensive approach to managing cyber security threats and vulnerabilities.

As we have seen from the Stuxnet malicious code, the capability and intent to launch targeted cyber attacks on critical infrastructure and other information technology exists. Public facing information systems are constantly under attack across all critical infrastructures. The absence of a successful attack on our Nation's electricity infrastructure may mean that electric power providers have been vigilant in protecting their systems, or it may be that adversaries have chosen not to attack at this time. Because of the dynamic nature of the threat environment and the variety of threat actors, it is challenging to know if and when an attack may occur on the grid. Thus, the electricity sector must be equipped to constantly adapt and defend their systems from this evolving threat.

DOE, in coordination with the National Institute for Standards and Technology (KIST), Department of Homeland Security (DHS), and NERC, is leading a public and private sector collaboration to develop a risk management process guideline to provide a consistent, repeatable, and adaptable process for the electric sector, and enable organizations to proactively manage cyber security risk. This guideline is an important step towards moving all organizations within the electricity sector towards a common risk management process. It incorporates risk assessments with ongoing monitoring, enabling organizations to quickly and effectively respond to cyber security threats and vulnerabilities.

Question 3. In previous hearings on cyber security in this Committee, we've heard about the efforts being made to work with our neighbors in Canada to ensure consistency in practices and procedure across the bulk power system. This cross-border collaboration is important to me since my state, New Hampshire, shares a border with Canada. Do the effects of cyber attacks cross boundaries? Would a successful attack on the Canadian power system have an effect in New Hampshire?

Answer. Yes, the effects of a cyber attack can cross boundaries. Eastern Canada and the eastern United States are electrically interconnected and thus the operations of power companies north of the border directly impact the operations of US power companies. Even though the control systems of the power companies run independently using different hardware architectures and different software, what happens to the grid on one side of the border can potentially impact the other side of the border. Power systems are designed and have safeguards to limit the impacts of any disruption. As an example of how these grids are operationally interconnected, in February of 2008, portions of the power grid in southeastern Florida shut down due to a fault at a single substation. This event in Florida was "felt" in Canada by way of frequency deviations in Canada.

Question 4. Could you elaborate about existing cooperation with Canada on protecting against vulnerabilities in the electric system?

Answer. The Department of Energy is partnering on a Department of Homeland Security led initiative with private, State and other Federal agencies to conduct a Cross Border Regional Resiliency Assessment Program (RRAP) focused on energy and transportation for Maine and New Brunswick, Canada. The RRAP is a cooperative, DHS-led assessment of specific critical infrastructure and regional analysis of the surrounding infrastructure to examine vulnerabilities, threats, and potential consequences from an all-hazards perspective to identify dependencies, interdependencies, cascading effects, resiliency characteristics, and gaps. The focus of this RRAP is on the critical regional and cross-border energy systems and assets, and their interdependencies, specifically with the Transportation Sector. International energy dependencies and impacts are being examined as well. The RRAP began in May 2011, with vulnerability assessments on Energy and Transportation assets scheduled to begin in July 2011. The final report is projected to be delivered in April 2012.

Power companies in the United States and in Canada are very active members of NERC and serve on the Critical Infrastructure Protection Committee. This committee is involved with many efforts to improve the reliability and security of the interconnected power grid through standards development, compliance enforcement, assessments of risk and preparedness. Canadian companies are active on several NERC task forces following up on the 2009 High Impact Low Frequency Event Risk to the North American Bulk Power System Workshop cosponsored by NERC and DOE.

Question 5. Are there procedures currently in place to share information about imminent threats across the border?

Answer. NERC currently disseminates critical information including threat information to power companies on both sides of the border. DHS and Public Safety Canada constantly monitor the threat landscape and provide NERC with threat information related to the electricity sector.

○