S. HRG. 111–29

CYBER SECURITY

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

TO

RECEIVE TESTIMONY ON A JOINT STAFF DRAFT RELATED TO CYBER SECURITY AND CRITICAL ELECTRICITY INFRASTRUCTURE

MAY 7, 2009

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

U.S. GOVERNMENT PRINTING OFFICE

50–179 PDF WASHINGTON : 2009

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*

BYRON L. DORGAN, North Dakota
RON WYDEN, Oregon
TIM JOHNSON, South Dakota
MARY L. LANDRIEU, Louisiana
MARIA CANTWELL, Washington
ROBERT MENENDEZ, New Jersey
BLANCHE L. LINCOLN, Arkansas
BERNARD SANDERS, Vermont
EVAN BAYH, Indiana
DEBBIE STABENOW, Michigan
MARK UDALL, Colorado
JEANNE SHAHEEN, New Hampshire

LISA MURKOWSKI, Alaska
RICHARD BURR, North Carolina
JOHN BARRASSO, Wyoming
SAM BROWNBACK, Kansas
JAMES E. RISCH, Idaho
JOHN MCCAIN, Arizona
ROBERT F. BENNETT, Utah
JIM BUNNING, Kentucky
JEFF SESSIONS, Alabama
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 7, 2009

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

The committee met, pursuant to notice, at 10 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. Recent newspaper headlines and television news coverage have highlighted the serious security threats to the electricity system in the country. The *Wall Street Journal* article talked about Soviet and Chinese hackers who may have left potentially damaging computer viruses in the control systems of electric utilities.

Just the thought that foreign agents are hacking into our control systems is obviously alarming and the potential for damage they could do or, in the case of a conflict would create a compelling reason to act to prevent that damage.

We recently sponsored a classified briefing for members and staff on this set of issues. Members of security agencies and the Department of Energy and the Federal Energy Regulatory Commission told us about these threats and about the inadequacy of our government's authority to respond to and prevent these threats.

Some thought that we had taken sufficient action to protect against these types of threats when we put into place the Reliability Protection Structure of section 215 of the Federal Power Act which we passed in 2005. More recently however, we have come to believe that these provisions do not provide sufficient protection against computer attacks. Both the recent Republican Chairman of the Federal Energy Regulatory Commission, Joe Kelliher, and the current Democratic Chair, Jon Wellinghoff, have indicated that they believe they need stronger authority to deal with cyber threats and vulnerabilities.

Almost all the witnesses gathered here today agree that we need some kind of increased Federal authority, although there is disagreement as to exactly what that authority should look like and who should exercise it. This hearing is on a bill that we intend to include in a comprehensive energy bill that the committee is working on to address these gaps in Federal authority and to protect against these dangers.

The proposal is fairly simple. It gives the Secretary of Energy authority to order actions to protect against imminent threats. When a security agency informs the Secretary that an action is about to take place, the Secretary is able to order measures to protect against the attack.

It then goes on to allow FERC to issue rules for longer-term circumstances that are not immediate threats, but that are too dangerous to wait for the development of orders through the extremely cumbersome NERC process. This authority does not supersede the NERC process. FERC can issue rules that can then be replaced by rules developed under the NERC process, when those rules finally are such that the Commission can approve them.

[The proposal referred to follows:]

CYBER SECURITY PROTECTION

STAFF DRAFT SUMMARY

MAY 1, 2009

Definitions

- Cyber Security Threat means the imminent danger of an act that disrupts or attempts to disrupt the operation of electronic devices or communications networks for the control of critical electric infrastructure.
- Cyber Security Vulnerability means a weakness or flaw in the design or operation of any programmable device or communication network that exposes critical electric infrastructure to a cyber security threat.

Authority of the Commission

- The Commission must promulgate rules or orders necessary to protect against cyber security vulnerabilities.
- The Commission may issue such rules without prior notice or hearing if it determines that the rule or order must be promulgated immediately to protect against a cyber security vulnerability.

Emergency Authority of the Secretary

- If immediate action is necessary to protect against a cyber security threat, the Secretary may require, by order, with or without notice, that entities subject to the jurisdiction of the Commission under this section, take such actions as are necessary to protect against that threat.
- The Secretary is encouraged to consult and coordinate with appropriate officials in Canada and Mexico.

Duration of Expedited or Emergency Rules or Orders

Rules or orders issued either by the Secretary under Emergency Authority, or the Commission under Expedited Procedures, remain effective for no more than 90 days, unless the Commission gives interested persons an opportunity to submit written comments and the Commission affirms, repeals or amends the rule or order.

Critical Electric Infrastructure Information

Critical electric infrastructure information is given the same protection as is contained in the Critical Infrastructure Information Act of 2002.

SEC.____. CRITICAL ELECTRIC INFRASTRUCTURE.

Part II of the Federal Power Act (16 U.S.C. 824 et seq.) is amended by adding at the end the following:

"SEC. 224. CRITICAL ELECTRIC INFRASTRUCTURE.

"(a) DEFINITIONS.—In this section:

"(1) CRITICAL ELECTRIC INFRASTRUCTURE.—The term 'critical electric infrastructure' means sys tems 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 inca-

pacity or destruction of the systems and as sets would have a debilitating impact on national se curity, national economic security, or national public health or safety.

"(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastruc ture information' means critical infrastructure infor mation relating to critical electric infrastructure.

"(3) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' has the meaning given the term in section 212 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 131).

"(4) CYBER SECURITY THREAT.—The term 'cyber security threat' means the imminent danger of an act that disrupts, attempts to disrupt, or poses a significant risk of disrupting the operation of pro grammable electronic devices or communications net works (including hardware, software, and data) es sential to the reliable operation of critical electric in frastructure.

"(5) CYBER SECURITY VULNERABILITY.—The term 'cyber security vulnerability' means a weakness or flaw in the design or operation of any program mable electronic device or communication network that exposes critical electric infrastructure to a cyber security threat.

"(6) SECRETARY.—The term 'Secretary' means the Secretary of Energy.

"(b) AUTHORITY OF COMMISSION.—

"(1) IN GENERAL.—The Commission shall pro mulgate or issue such rules or orders as are nec essary to protect critical electric infrastructure from cyber security vulnerabilities.

"(2) EXPEDITED PROCEDURES.—The Commission may promulgate or issue a rule or order without prior notice or hearing if the Commission determines the rule or order must be promulgated or issued im mediately to protect critical electric infrastructure from a cyber security vulnerability.

"(c) EMERGENCY AUTHORITY OF SECRETARY.—

"(1) IN GENERAL.—If the Secretary determines that immediate action is necessary to protect critical electric infrastructure from a cyber security threat, the Secretary may require, by order, with or without notice, persons subject to the jurisdiction of the Commission under this section to take such actions as the Secretary determines will best avert or miti gate the cyber security threat.

"(2) COORDINATION WITH CANADA AND MEXICO.—In exercising the authority granted under this subsection, the Secretary is encouraged to consult and coordinate with the appropriate officials in Can ada and Mexico responsible for the protection of cyber security of the interconnected North American electricity grid.

"(d) DURATION OF EXPEDITED OR EMERGENCY RULES OR ORDERS.—Any rule or order promulgated or issued by the Commission without prior notice or hearing under subsection (b)(2) or any order issued by the Sec retary under subsection (c) shall remain effective for not more than 90 days unless, during the 90 day-period, the Commission—

"(1) gives interested persons an opportunity to submit written data, views, or arguments (with or without opportunity for oral presentation); and

"(2) affirms, amends, or repeals the rule or order.

"(e) JURISDICTION.—

"(1) IN GENERAL.—Notwithstanding section 201, this section shall apply to any entity that owns, controls, or operates critical electric infrastructure.

"(2) COVERED ENTITIES.—

"(A) IN GENERAL.—An entity described in paragraph (1) shall be subject to the jurisdic tion of the Commission for purposes of—

"(i) carrying out this section; and

"(ii) applying the enforcement authorities of this Act with respect to this section.

"(B) JURISDICTION.—This subsection shall not make an electric utility or any other entity subject to the jurisdiction of the Commission for any other purpose.

"(f) PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—Section 214 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 133) shall apply to critical electric infrastructure information submitted to the Commission or the Secretary under this section to the same extent as that section applies to critical infrastructure information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 131 et seq.).".

This is obviously an important issue and one that I hope we are able to deal with as part of an energy bill, and I thank the witnesses for being here.

Let me go ahead and introduce the witnesses and then we will hear the testimony.

Patricia Hoffman is Principal Deputy and Acting Assistant Secretary in the Office of Electricity Delivery and Energy Reliability at the Department of Energy. She's been here before our committee recently on other issues as well.

Joseph McClelland is the Director of the Office of Electric Reliability at FERC and thank you for being here.

Rick Sergel is President and CEO of the North American Electric Reliability Corporation in Princeton. Thank you for being here. Allen Mosher is a Senior Director of Policy Analysis and Reliability with the American Public Power Association.

David Owens is the Executive Vice President of Business Operations with Edison Electric Institute. Thank you very much for being here.

If each of you can take 5 or 6 minutes and give us your perspective on this set of issues and then we will undoubtedly have questions.

Ms. Hoffman.

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

Ms. HOFFMAN. Thank you. Mr. Chairman and members of the committee. Thank you for this opportunity to testify before you on cyber security issues facing the electric industry and on emergency authorities to protect critical electric infrastructure.

All of us here today share common concerns that vulnerabilities exist within the electric system and that the government and private sector must do everything we can to address it. This is particularly true for Smart Grid systems which, by their very nature, involve the use of information technologies in areas and applications on the electric system where they not have been used before.

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

Our efforts to enhance the cyber security of the energy infrastructure have produced results in five areas. We have identified cyber vulnerabilities in energy control systems and worked with vendors to develop hardened systems that mitigate the risks. We

have developed more secure communication methods between energy control systems and field devices. We have developed tools and methods to help utilities assess their security posture. We have developed modeling and simulation capabilities to estimate the effects of cyber attacks on the power grid. Finally, we have provided extensive cyber security training for the energy asset owners and operators to help them prevent, detect, and mitigate cyber penetration.

In 2005, the Department worked closely with asset owners and operators in the oil, gas, and electric sectors to develop a roadmap to secure control systems in the energy sector. The roadmap is a detailed, prioritized plan for cyber security improvements over the next 10 years including best practices, new technologies, and risk management. The Roadmap vision is that control systems for critical applications will be designed, installed, and operated to maintain and survive an intentional cyber assault with no loss of critical function.

Efforts at the national labs are producing results that industry can use today to enhance the security of their control systems. For example, Sandia National Laboratories developed an Advanced Network Toolkit For Assessments and Remote Mapping which aids utility owners in mapping access points to allow easy visualization of their control system networks, an important critical step in meeting the North American Electric Reliability Corporation's critical infrastructure protection standard. Through the Department's National Supervisory Control and Data Acquisition Test Bed program, we have assessed 90 percent of the current market offerings of SCADA and energy management systems in the electric sector and 80 percent of the current market offerings in the oil and gas sector. Twenty test bed and offsite assessments of control systems from vendors have led to the development of 11 hardened control system designs with 31 of these systems now deployed in the marketplace.

The national labs also educate end-users on cyber security best practices and implementing methods to better manage control system risks. For example, the Idaho National Laboratory has released a common vulnerabilities report. This report represents the steadily growing understanding of control system security issues and methods for mitigating current and emerging vulnerabilities. This effort is expanding to new technologies; such as substation automation and the Smart Grid, as the program seeks a continuing understanding of the systems being planned for and developed for the energy sector critical infrastructure.

The Department is also working to implement Smart Grid Investment Grand and Demonstration Programs under the American Recovery and Reinvestment Act of 2009. These programs are authorized under title 13 of the Energy Independence and Security Act of 2007 for the Smart Grid. We are hoping to implement these programs in a responsible manner and the request for proposals for Smart Grid projects will include requirements that each applicant will thoroughly and systematically address all cyber security risks to their systems.

A key component of the Smart Grid is the Advanced Metering Infrastructure, or AMI. AMI requires two-way communications be-

tween utilities and the end-users. Over the last 10 months, DOE has been partnering with the AMI Security Task Force under the Utility Communications Architecture International Users Group. This task force is comprised of utilities, security domain experts, standard body representatives, and industry vendors.

On March 10, 2009, the task force published the AMI security requirements which provides critical guidance for vendors and utilities to design and procure secure, reliable AMI systems. Because of the success of this industry-government collaboration, the Department is working with the task force to expand the activity and develop a suite of security requirements for all critical Smart Grid applications. The National Institute of Standards and Technology is responsible for developing a framework for interoperability standards development for the Smart Grid. These standards will be submitted to the Federal Energy Regulatory Commission for rulemaking.

The Department views the development of interoperability standards that includes appropriate cyber security protections as one of the key milestones toward realizing the goal of widespread implementation of Smart Grid technologies, tools, and techniques.

With regard to protecting the electric grid from newly discovered vulnerabilities, the Department does not have a position on the Draft Joint Cyber Security Text. The Department does provide the following technical comment: All vulnerabilities must be thoroughly evaluated on a scientific basis to determine the impact and risk to the Nation in the event the vulnerability was to be exploited. Any decision to act or to issue an order by the government must be based on sound risk management principles and judgment, considering the characteristics of the vulnerability, the capabilities of the threat, the likelihood of attack, the consequences to the Nation should the vulnerability be exploited, and the cost of mitigation.

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

[The prepared statement of Ms. Hoffman follows:]

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

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

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

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

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

For example, Wide Area Measurement Systems (WAMS) technology is based on obtaining high-resolution power system measurements (e.g., voltage) from sensors that are dispersed over wide areas of the grid. The data is synchronized with timing signals from Global Positioning System (GPS) satellites. The real-time information available from WAMS allows operators to detect and mitigate a disturbance before it can spread and enables greater utilization of the grid by operating it closer to its limits while maintaining reliability. When Hurricane Gustav came ashore in Louisiana in September 2008, an electrical island was formed in an area of Entergy's service territory. Entergy used the phasor measurement system to detect this island, and the phasor measurement units (PMU) in the island to balance generation and load for some 33 hours before surrounding power was restored.

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

DEPARTMENT OF ENERGY ACTIVITIES

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

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

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

As a result, the Department was one of the first research organizations to align its cyber security research activities with the Roadmap goals and vision. The Institute for Information Infrastructure Protection (I3P) is working to develop several technologies that address Roadmap goals including security metrics and trusted devices. The Trusted Cyber Infrastructure for the Power Grid (TCIP) (a collaboration of universities led by the University of Illinois at Champaign-Urbana working with energy sector asset-owners and operators and vendors with funding from NSF, DOE, and DHS) is also conducting extensive cyber security research that aligns with the Roadmap goals. In addition, there are over 50 other public and private organizations working on projects that directly address the challenges identified in the Roadmap.

Efforts at the national labs are also producing results that industry can use today to enhance the security of their control systems. For example, Sandia National Laboratories developed the Advanced Network Toolkit for Assessments and Remote

Mapping, or ANTFARM. This tool aids energy utility owners in mapping critical cyber assets and access points to allow easy visualization of their control system networks-a critical step in meeting the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards. Released in August 2008. The toolkit is open source and available online for free.

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

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

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

The Department has also funded several research and development projects with the private sector. The Bandolier project, led by Digital Bond, is developing security audit files, which are incorporated into a utility's existing network scanners and used to audit the control system's security settings against an optimal security configuration. Given that large control systems can have over 1000 security settings, Bandolier can help a utility enhance its security posture while saving time and money at the same time. Audit files are now available for Siemens, Telvent, and ABB. Digital Bond has made its product available for a nominal subscriber fee on its website.

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

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

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

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

goes beyond stopping traditional threats to rendering both traditional and new threats harmless.

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

SMART GRID

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

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

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

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

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

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

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

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

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

The CHAIRMAN. Thank you very much.

Mr. McClelland.

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 invitation to appear before you today to discuss the cyber security of the electric 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.

Although new section 215 of the Federal Power Act has provided an adequate foundation for the development of reliability standards to date, the threat of cyber attacks or other intentional malicious acts against the electric grid is very different. These threats can endanger national security and they may be posed by foreign nations or others intent on attacking the United States through the electric grid. Widespread disruption of electric service could quickly undermine the U.S. Government, its military, and the economy, as well as endanger the health and safety of millions of our citizens.

Given the national security dimension to this threat, there may be a need to act quickly to protect the grid and to act in a manner where action is mandatory, rather than voluntary, and to protect certain information from public disclosure. Faced with the cyber or other national threat to reliability, there may be a need to act decisively in hours or days, rather than weeks, months, or years.

The Commission's legal authority is inadequate for such action, as it is required to depend upon the Electric Reliability Organization, or ERO, to develop and propose standards to address cyber security issues. The process employed by the ERO typically takes years to develop the standard, is open to public review, and may not be necessarily responsive to the Commission's directives. This is true of both cyber and non-cyber threats that pose national security concerns.

In the case of such threats to the electric system, the Commission does not have timely, confidential, or direct authority to protect the reliability of the system. As a result, I believe legislation is needed. Any new legislation should address several key concerns.

First, the legislation should allow the Commission to take action before a cyber or other national security incident has occurred. Second, any legislation should allow the Commission to maintain the appropriate confidentiality of any security-sensitive information submitted or developed through the exercise of this authority.

Third, it is important that Congress be aware that if additional reliability authority is limited to the "bulk power system", as defined in the Federal Power Act, it would exclude protection against attacks involving Alaska and Hawaii and possibly the territories, including any Federal installations located therein. In addition, the current interpretation of bulk power system also would exclude some transmission and all local distribution facilities, including virtually all of the grid facilities in large cities such as New York City;

thus precluding possible Commission action in these population centers.

Finally, legislation should not only address cyber security threats, but also other national security threats to reliability.

The Joint Staff favors one approach that would largely rectify the inadequacies in existing Federal authority to address cyber threats to the electric grid. It gives the Commission authority to issue rules or orders that are necessary to protect critical electric infrastructure and thus allow the Commission to act to protect against damage to the grid.

I will briefly point out a few concerns with the joint staff draft. While the draft bill addresses the protection of critical infrastructure information, it could be construed to provide protection only for information voluntarily submitted to the Commission or the Secretary. It does not address other information, such as that which may be compelled or developed by the Commission or the Secretary, or information that would be included in orders issued by either agency. Therefore, I recommend that the language be amended to address these issues.

I also recommend that the legislation address not only cyber security threats, but other national security threats to reliability. Potential physical acts against the grid can cause equal or greater destruction than cyber attacks and the Federal Government should have no less ability to act to protect against such damage.

Finally, Congress should be aware that if additional liability authority is limited to the areas within the Commission's jurisdiction under section 215 of the Federal Power Act, it would exclude protection against reliability threats in Alaska, Hawaii, and possibly the territories. Again, including any Federal installations located therein as well as major population areas such as New York City.

Thank you again for the opportunity to testify today and I would be happy to answer any questions they you may 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 cyber 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 in the area of security, some of the Commission's actions to implement section 215 of the Federal Power Act, and some of the limitations in the Commission's authority. The Commission does not have sufficient authority to provide effective protection of the grid against cyber attacks or other security threats to reliability. As will be explained in more detail later, this is primarily due to three factors regarding the development of reliability standards under section 215; lack of timeliness, lack of ability to protect security-sensitive information, and lack of ability to control the content of proposed cybersecurity standards. Therefore, legislation is needed and my testimony discusses the key elements that should be included in any new legislation in this area.

BACKGROUND

In the Energy Policy Act of 2005 (EPAct 2005), the 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 reliability standards apply to the users, owners and operators of the bulk power system and become mandatory 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 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. The Commission however, does not have the authority to modify or author a standard but must depend upon the ERO to do so.

The Commission has implemented section 215 diligently. Within 180 days of enactment, the Commission adopted rules governing the reliability program. In mid-2006, it approved the North American Electric Reliability Corporation (NERC) as the ERO. In March 2007, the Commission approved the first set of national mandatory and enforceable reliability standards. In April 2007, it approved eight regional delegation agreements to provide for development of new or modified standards and enforcement of approved standards by Regional Entities.

In exercising its new authority, the Commission has interacted extensively with NERC and the industry. The Commission also has coordinated with other federal agencies, such as the Department of Homeland Security, the Department of Energy, the Nuclear Regulatory Commission, and the Department of Defense. Also, the Commission has established regular communications and meetings with regulators from Canada and Mexico regarding reliability, since the North American bulk power system is an interconnected continental system subject to the varied regulatory regimes of three nations.

CYBER SECURITY STANDARDS APPROVED UNDER SECTION 215

An important part of the Commission's responsibility to oversee the development of reliability standards involves cyber security. Section 215 defines "reliability standard[s]" as including requirements for the "reliable operation" of the bulk power system including "cybersecurity protection." Section 215 defines reliable operation to mean operating the elements of the bulk power system within certain limits so instability, uncontrolled separation, or cascading failures will not occur "as a result of a sudden disturbance, including a cybersecurity incident."

Section 215 also defines a "cybersecurity incident" as a "malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."

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. Each of these standards contains layers of multiple requirements. 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." NERC proposed an implementation plan under which certain requirements would be "auditably compliant" beginning by mid-2009, and full compliance with the CIP standards would not be mandatory until 2010.

On January 18, 2008, after issuing both a staff preliminary assessment and notice of proposed rulemaking, the Commission issued a Final Rule approving the CIP Reliability Standards and concurrently directed NERC to develop significant modifications addressing specific concerns, such as the breadth of discretion left to utilities by the standards. For example, the standards state that utilities "should interpret and apply the reliability standard[s] using reasonable business judgment." Simi-

larly, the standards at times require certain steps "where technically feasible," but this is defined as not requiring the utility "to replace any equipment in order to achieve compliance." Also, the standards would allow a utility at times not to take certain action if the utility documents its "acceptance of risk" that might be placed on the bulk-power system. To address this, the Final Rule directed NERC, among other things: (1) to develop modifications to remove the "reasonable business judgment" language and the "acceptance of risk" exceptions; and, (2) to develop specific conditions that a responsible entity must satisfy to invoke the "technical feasibility" exception. NERC and the industry are working on proposed modifications to address these two issues. However, until such time as the standards are modified by the ERO through its stakeholder process, approved by the Commission, and implemented by industry, the discretion remains and critical facilities will be left unprotected.

A good example of the discretion implicit in the existing cyber security standards involves the utility's ability to determine which of its facilities would be subject to them. In the Final Rule, the Commission addressed its concerns by requiring 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 is subject to approval by the affected stakeholders in the standards development process and therefore has not yet been presented to the Commission. NERC recently conducted a survey on this issue which seems to validate the Commission's concern and original directives by demonstrating that a significant percentage of owners and operators do not believe they own or operate critical cyber assets. For example, NERC stated that only 29% of generation owners and generation operators reported at least one critical asset, though it is unclear from NERC's data what portion of the Nation's generation capacity that 29% represents, or what portion the designated critical assets represent. Thus, it is not clear, even today, what percentage of critical assets and their associated critical cyber assets has been identified. It is clear, however, that this issue is serious and represents a significant gap in cybersecurity protection.

CURRENT PROCESS TO ADDRESS CYBER OR OTHER NATIONAL SECURITY THREATS TO RELIABILITY

As an initial matter, it is important to recognize how mandatory reliability standards are established under section 215. Under section 215, reliability standards are 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 takes years to develop standards for the Commission's review. In fact, the cyber security standards approved by FERC took the industry approximately three years to develop.

NERC's procedures for developing standards allow extensive opportunity for industry 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 the standard and on the substance of the proposed standard. Although inclusive, the process is relatively slow, cumbersome and unpredictable regarding its responsiveness to the Commission's directives.

Key steps in the NERC process include: nomination of a proposed standard using a Standard Authorization Request (SAR); public posting of the SAR for comment; review of the comments by industry volunteers; drafting or redrafting of the standard by a team of industry volunteers; public posting of the draft standard; field testing of the draft standard, if appropriate; formal balloting of the draft standard, with approval requiring a quorum of votes by 75 percent of the ballot pool and affirmative votes by two-thirds of the weighted industry sector votes; re-balloting, if negative votes are supported by specific comments; approval by NERC's board of trustees; and an appeals mechanism to resolve any complaints about the standards process. NERC-approved standards are then submitted to the Commission for its review. This standards development process requires public disclosure regarding the reason for the proposed standard, the manner in which the standard will address the issues at-hand, and any subsequent comments and resulting modifications in the standards as the affected stakeholders review the material and provide comments.

Generally, the procedures used by NERC are appropriate for developing and approving 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 as it relates to most reliability standards. 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 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. If a significant vulnerability in the bulk power system is identified, procedures used so far for adoption of reliability standards take too long to implement effective corrective steps.

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 cyber security or other 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, would widely publicize both the vulnerability and the proposed solutions, thus increasing the risk of hostile actions before the appropriate solutions are implemented.

In addition, the proposed standard submitted to the Commission may not be sufficient to address the vulnerability or threat. As noted above, when a proposed reliability standard is submitted to FERC for its review, whether submitted under the urgent action provisions or the usual process, the agency cannot modify such standard and must either approve or remand it. Since the Commission may not modify a proposed reliability standard under section 215, it 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.

Finally, the open and inclusive process required for standards development is not consistent with the need to contain security-sensitive information. For instance, a SAR would normally detail the need for the standard as well as the proposed mitigation to address the issue. Subsequent drafts of the standard would consider how effectively it addresses the cyber security matters and what objections or revisions are proposed by the stakeholders resulting in a final version that would be filed with the Commission for review. Potential adversaries would have the ability to monitor these developments and alter their actions as necessary to preserve an effective attack vector.

NERC'S "AURORA" ADVISORY AND SUBSEQUENT ACTIONS

Currently, the alternative to a mandatory reliability standard is for NERC to issue an advisory encouraging utilities and others to take voluntary action to guard against cyber or other vulnerabilities. That approach provides for quicker action, but any such advisory is not mandatory, and should be expected to produce inconsistent and potentially ineffective responses. That was the Commission's experience with the response to an advisory issued in 2007 by NERC regarding an identified cyber security threat referred to as the "Aurora" threat. While NERC can issue an alert, as it did in response to the Aurora vulnerability, compliance with these alerts is voluntary and subject to the interpretation of the individual utilities. Also, an alert can be general in nature and lack specificity. For example, as Commission staff has found with the Aurora alert, such alerts can cause uncertainty about the specific strategies needed to mitigate the identified vulnerabilities and the assets to which they apply. Reliance on voluntary measures to assure national security is fundamentally inconsistent with the conclusion Congress reached during enactment of EPAct 2005, that voluntary standards cannot assure reliability of the bulk power system.

Damage from cyber attacks could be enormous. All of the electric system is potentially subject to cyber attack, including power plants, substations, transmission lines, and local distribution lines. A coordinated attack could affect the electrical grid to a greater extent than the August 2003 blackout and cause much more extensive damage. Cyber attacks can physically damage the generating facilities and other equipment such that restoration of power takes weeks or longer, instead of

a few hours or days. The harm could extend not only to the economy and the health and welfare of our citizens, but even to the ability of our military forces to defend us, since many military installations rely on the bulk power system for their electricity. In fact, a recent Defense Science Board report concluded that "critical missions at military installations are vulnerable to loss from commercial power outage and inadequate backup power supplies."[1] The cost of protecting against cyber attacks is difficult to estimate but, undoubtedly, is much less than the damages and disruptions that could be incurred if we do not protect against them.[2]

The need for vigilance may increase as new technologies are added to the bulk power system. For example, "smart grid" technology will provide significant benefits in the use of electricity. These include the promised ability to manage not only energy sources but also energy consumption. However, a smarter grid would permit two-way communication between the electric system and a much larger number of devices located outside of controlled utility environments, which will introduce many potential access points. To some degree, this is similar to the banking industry allowing its customers to bank on line, but only with appropriate security protections in place. Security features must be an integral consideration, as the Commission stated in a recent proposed policy statement on smart grid. As the "smart grid" effort moves forward, steps will need to be taken to ensure that cyber security protections are in place prior to its implementation. 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.

KEY ELEMENTS OF NEEDED LEGISLATION

In my view, section 215 provides an adequate statutory foundation for the ERO to develop reliability standards for the bulk power system. However, the threat of cyber attacks or other intentional malicious acts against the electric grid is different. These are national security threats that may be posed by foreign nations or others intent on attacking the U.S. through its electric grid. The nature of the threat 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 legal authority is inadequate for such action. This is true of both cyber and non-cyber threats that pose national security concerns. In the case of such threats to the electric system, the Commission does not have sufficient authority to timely protect the reliability of the system.

Any new legislation should address several key concerns. First, legislation should allow the Commission to take action before a cyber or other national security incident has occurred to prevent a significant risk of disruption to the grid due to such an incident. In order to protect the grid, it is vital that the Commission be authorized to act before an attack. Second, any legislation should allow the Commission to maintain appropriate confidentiality of any security-sensitive information submitted or developed through the exercise of this authority. It should also allow the Commission to protect such information when the Commission issues orders under any new authority. Third, it is important that Congress be aware that if additional reliability authority is limited to the "bulk power system," as defined in the FPA, it would exclude protection against attacks involving Alaska and Hawaii and possibly the territories, including any federal installations located therein. The current interpretation of "bulk power system" also would exclude some transmission and all local distribution facilities, including virtually all of the grid facilities in large cities such as New York., thus precluding possible Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population areas. Finally, legislation should address not only cyber security threats but also other national security threats to reliability.

The Joint Staff draft bill is one approach that would largely rectify the inadequacies in existing federal authority to address cyber threats to the electric grid. It gives the Commission authority to issue rules or orders that are necessary to protect

[1] Report of the Defense Science Board Task Force on DoD Energy Strategy "More Fight—Less Fuel", February 2008.

[2] As an example, the US Canada Joint Task Force on the August 2003 Blackout concluded that the outage that affected over 50,000,000 citizens and was estimated to cost between $4 and $10 billion dollars in the United States.

critical electric infrastructure from weaknesses or flaws in the design or operation of electric devices or networks that expose critical electric infrastructure to a cyber security threat. This authority to address cyber security vulnerabilities would apply to all systems or assets, whether physical or virtual, used for the generation, transmission, and distribution of electric energy that in the determination of the Commission are so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on the security, national economic security, or national public health or safety. Thus, it would allow the Commission to act to protect against potential damage to the grid, including the grid facilities in New York City, which I referenced earlier.

As I have noted, a key concern with respect to any cyber security legislation is that the Commission must be allowed to maintain appropriate confidentiality of any security-sensitive information submitted or developed through the exercise of its authority. This applies to information submitted to the Commission and to orders issued by the Commission, which may contain security-sensitive information. While the draft bill addresses the protection of critical infrastructure information, it could be construed to provide protection only for information voluntarily submitted to the Commission or the Secretary. Not all information submitted to the Commission or the Secretary will be submitted voluntarily, but rather may be ordered to be submitted in an agency rule or order. Additionally, the Commission or the Secretary may need to include sensitive information in the orders they issue and this information similarly should be non-public. Therefore, I recommend that the language be amended to address these issues.

I also recommend that the Joint Staff draft be amended to address not only cyber security threats but also other national security threats to reliability. Intentional physical malicious acts (targeting, for example, critical substations and generating stations) 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. 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, but the Commission has unique expertise regarding the reliability of the grid, the consequences of threats to it and the measures necessary to safeguard it. If particular circumstances cause both FERC and other governmental authorities to require action by utilities, FERC will coordinate with other authorities as appropriate.

Finally, Congress should be aware of the fact that if additional reliability authority is limited to the areas within the Commission's jurisdiction under section 215 of the FPA, it would exclude protection against reliability threats in Alaska and Hawaii and possibly the territories, including any federal installations located therein.

CONCLUSION

The Commission's 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. 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. Sergel, go right ahead.

STATEMENT OF RICHARD P. SERGEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Mr. SERGEL. Thank you, Chairman, and members of the committee. I appreciate the opportunity to testify today and I commend you and your staffs for your attention to this important issue.

NERC is committed to ensuring the reliability of the bulk power system in North America in the face of cyber security threats and assuring that NERCs efforts will complement those of the government and industry in regard to cyber security protection and assuring that there are no gaps, and that that responsibility is clear for execution of cyber security protection initiatives.

Now, as the international regulatory authority for the reliability of the bulk power system in North America, NERC is responsible

for developing reliability standards applicable to all users and owners of the system, ensuring that each of the nearly 2,000 entities that own and operate components of the system understand cyber security and the efforts needed to adequately protect the security of the bulk power system, and this has been a priority for us.

Now, my written testimony details the steps NERC has taken to enhance protection of the system from cyber security vulnerabilities and threats. I'm not going to talk about those here today. We do have eight of the mandatory and enforceable reliability standards in effect today, focus on cyber security, and fill a specific role in the protection of the system. Now, these standards were developed under the process established in section 215, a process that worked to put those standards in place for securing the grid and and we are working today to improve those standards.

But reliability standards are not enough. NERC agrees that new specific authority for emergency response to cyber threats is necessary. In the case of an imminent cyber security threat, authority to direct action should be vested in the Federal Government in the United States and, as appropriate, in Canada.

The Joint Staff Draft addresses what we see as the principle gap in the current law. The Federal Government lacks sufficient authority to act to address an imminent and specific cyber security threat to the critical infrastructure of the United States. NERC believes that authority to act in such emergencies should be assigned to a single Federal agency.

The Draft would give the Secretary of Energy the authority to act in such circumstances. The provisions of the Draft to encourage consultation and coordination with officials in Canada and Mexico are, we believe, very important in recognition of the international nature of the interconnected North American power system.

Now, in addition to the new authority in the Department of Energy, the Draft would also give new authority to the Federal Energy Regulatory Commission to establish standards to address not only emergencies, but cyber security vulnerability. Moreover, FERC would be authorized to adopt rules or orders without notice or hearing.

NERC believes it would be unwise to supplant section 215, with respect to the establishment of cyber security standards and, whatever occurs, we need to make sure that it's complementary to what we do today. Hopefully we will be able to do that.

The NERC standard setting process brings together industry and security experts to develop standards that must apply to the international, interconnected grid. Developing long-term standards that apply to the more than 1,800 diverse entities that own and operate the grid is a complex undertaking.

Standards must apply equally to companies with thousands of employees and to those with only 20. Additionally, the standards must do no harm. They must take into account the unique component configurations and operational procedures that differ widely across the grid. Given the industry's extensive experience in standard development, NERC firmly believes that the level of expertise necessary to create standards that achieve security objectives and ensure liability can best be found within the industry itself. But I

emphasize again, that is only if we have emergency authorization in place.

Now, we are also concerned that the draft sets up potentially competing emergency authorities between the Secretary of Energy and FERC.

Now in closing, I'd like to reiterate our primary message. In the case of an imminent cyber security threat, the U.S. Government should be authorized to act immediately. With emergency responsibility in the hands of government, NERC would be better able to do what it does best, develop and implement cyber security reliability standards that will harden the grid against intrusion and aid in responding effectively to cyber security incidents.

Thank you.

[The prepared statement of Mr. Sergel follows:]

PREPARED STATEMENT OF RICHARD P. SERGEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

INTRODUCTION

The cyber security of the bulk power system in North America remains an important concern for our nation. When I last spoke in front of a Congressional committee in September 2008, my organization, the North American Electric Reliability Corporation (NERC), had just launched a major initiative to improve its response to cyber security challenges. I am pleased to report significant progress on this front, which is a clear indication that the framework established under Section 215 of the Federal Power Act is producing results. But I remain firm in the message I communicated nine months ago: the Federal government should be given additional, carefully crafted, emergency authority to address specific, imminent cyber security threats.

My testimony today will focus on the steps NERC has taken to enhance protection of the North American bulk power system from cyber security threats, and offer NERC's views on the Joint Staff Draft, which would provide the needed federal authority.

I. ROLE OF NERC STANDARDS IN PROTECTING THE BULK POWER SYSTEM FROM CYBER ATTACK

As the international regulatory authority for the reliability of the bulk power system in North America, NERC is responsible for developing Reliability Standards applicable to all users, owners and operators of the Bulk Power System. In the United States, NERC was certified as the Electric Reliability Organization by the Federal Energy Regulatory Commission (FERC) under Section 215 of the Federal Power Act in July 2006. NERC is similarly recognized in much of Canada, with the goal of ensuring that the entire interconnected power system operates from a single platform of sound reliability practices and procedures. NERC's over 100 Reliability Standards cover long-term reliability issues ranging from vegetation management to system operator training to modeling of the bulk power system.

Eight of NERC's standards are focused on cyber security and fill a specific role in the protection of the bulk power system. The standards are comprised of roughly forty specific requirements designed to lay a solid foundation of sound security practices that, if properly implemented, will develop the capabilities needed to secure critical infrastructure from cyber security threats. Audits of compliance with certain requirements included in the standards currently in effect, as approved by FERC on January 18, 2008 in Order No. 706, will begin on July 1, 2009.

NERC and its stakeholders recognize that the cyber security standards currently in effect can be improved and are actively working to do so in an expedited manner. As part of these efforts, NERC has worked with industry, consumer representatives and regulators to strengthen the standards both in the short-term by means of an initial six-month revision phase, and the longer-term, through a concurrent 18-month revision phase. Phase I revisions are already complete—they were adopted by the electric industry with an 88% approval rating last week and approved by NERC's Board of Trustees yesterday. The enhanced cyber security standards will be filed with FERC for approval promptly. We will also be filing those standards with authorities in Canada. Our work to further strengthen the cyber standards will

continue, and we look forward to bringing these revisions to FERC for approval in early 2010.

One of the areas NERC and its stakeholders are working to address in the longer-term revisions was the subject of an April 7 letter from NERC Chief Security Officer Michael Assante to industry stakeholders. The letter addressed the identification of Critical Assets and associated Critical Cyber Assets that support the reliable operation of the bulk power system, as required by NERC Reliability Standard CIP-002-1.[1] In the letter, Mr. Assante called on users, owners, and operators of the bulk power system to take a fresh look at current risk-based assessment models to ensure they appropriately account for new considerations specific to cyber security, such as the need to consider misuse of a cyber asset, not simply the loss of such an asset. The letter is part of the iterative process between NERC and industry stakeholders as we work together to improve reliability. In this case, NERC gathered information about the status of implementation of the critical infrastructure protection standards and fed that information and its own insights back to the industry as part of a cycle of continuous improvement.

This effort demonstrates that NERC is working to address a critical element of the cyber security challenge: the educational learning curve and resulting compliance-related challenges that must be addressed to improve the cyber security of the Bulk Power System. Ensuring that each of the nearly two thousand entities that own and operate components of the bulk power system understands cyber security and the efforts needed to adequately protect the security of the bulk power system has been a priority for NERC. While efforts such as the September 23rd, 2008 cyber security summit and classified briefings for industry executives have been important components of NERC's educational efforts, the standards development process itself has contributed a great deal to raising the profile and priority of cyber security within the electric sector. Other educational efforts currently under development include a series of webinars on compliance with the critical infrastructure protection standards and further regular communication with the industry.

At the end of the day, however, preparedness efforts like those discussed above are necessary but not sufficient to protect the system against specific and imminent threats. Protecting the system from these kinds of threats is dependent in large measure on the quality and timeliness of threat analysis and risk information developed by intelligence and law enforcement professionals and, importantly, their ability to share specific, actionable information with asset owners.

II. ADDRESSING IMMINENT AND SPECIFIC CYBER SECURITY THREATS

At NERC, we are working in a number of areas to help provide or assist in the provision of the kinds of information that will help the industry better secure critical assets from advanced, well-resourced threats and other known cyber activity on an ongoing basis. Strong and proactive participation by industry volunteers thus far has been encouraging.

In these efforts, NERC collaborates with the U.S. Department of Energy (DOE) and U.S. Department of Homeland Security (DHS) on critical infrastructure and security matters on an almost daily basis. Additionally, NERC serves as the Electricity Sector Information Sharing and Analysis Center (ES-ISAC),[2] which is responsible for promptly analyzing and disseminating threat indications, analyses and warnings to assist the electricity industry.

NERC disseminates these findings via its voluntary alerts mechanism, which has pioneered outreach to asset owners and is virtually unmatched by other infrastructure sectors. NERC is now able to provide timely critical reliability information to security and grid operations professionals, and has demonstrated success by conducting training and using the system to send alerts, record acknowledgements and receive responses within several days. As a result, our last recommendation was met with a 94 percent response rate. The industry has been very supportive as we have worked to improve this process. We look forward to launching an improved secure "alerts portal" to continue to improve this system in the coming weeks.

---

[1] The letter is available from the NERC website: http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf.

[2] The ES-ISAC has been operated by NERC since it was formed in 2001. The ES-ISAC was created as a result of action by the U.S. Department of Energy in response to Presidential Decision Directive 63 issued in 1998. The ES-ISAC works with the electricity industry to identify and mitigate cyber vulnerabilities by providing information, recommending mitigation measures, and following up to monitor implementation of recommended measures. NERC, in its capacity as the ES-ISAC, also has some related responsibilities for cyber and physical security issues associated with all electric facilities operated in the United States.

Other efforts underway at NERC include ongoing work with industry experts to assess security risks to the bulk power system of North America. Through these assessments, NERC seeks to broaden the understanding of cyber risk concerns facing the interconnected bulk power system and guide industry-wide efforts to develop prudent approaches to address the most material risks—in both the short-term, through appropriate alerts, and longer-term, through appropriate standards. Generalized and aggregated findings generated through these assessments will be communicated with asset owners through the voluntary alerts mechanism discussed above.

We firmly believe, however, that there are circumstances where these efforts will not be adequate to identify or address specific imminent threats. NERC agrees that new, specific authority for emergency response to cyber threats is necessary. In the case of an imminent cyber security threat, authority to direct action should be vested in the Federal government in the United States and as appropriate in Canada.

III. COMMENTS ON JOINT STAFF DRAFT

The Joint Staff Draft legislation would add a new Section 224, "Critical Electric Infrastructure," to the Federal Power Act. The draft addresses the principal gap that NERC sees in the current law: the Federal government lacks sufficient authority to act to address an imminent and specific cyber security threat to the critical infrastructure of the United States. NERC believes that authority to act in such emergencies should be assigned to a single Federal agency. Proposed Section 224(c)(1) does this by giving the Secretary of Energy the authority to act in such circumstances. Proposed Section 224(c)(2) properly encourages the Secretary, in exercising that authority, to consult and coordinate with appropriate officials in Canada and Mexico. This encouragement is entirely appropriate, because the bulk power system in North America comprises an interconnected grid that spans two international borders.

The draft legislation goes beyond the scope of Section 215, which specifically limits its standard-setting authority to apply only to users, owners, and operators of the bulk power system. The draft legislation would extend jurisdiction, for purposes of Section 224, to any entity that owns, controls, or operates systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce. At the time Congress adopted Section 215 of the Federal Power Act, providing for mandatory and enforceable reliability standards, it carefully chose the scope of jurisdiction it was granting, based on the nature of the risk and the international nature of the interconnected grid. Congress should again weigh the benefits and risks of broader jurisdiction as it considers this grant of additional authority.

Proposed Section 224(b) would give FERC authority to establish standards to address not only emergencies, but any cyber security vulnerability, defined as a weakness or flaw in the design or operation of any programmable electronic device or communication network that exposes critical electric infrastructure to a cyber security threat. It would authorize FERC to adopt rules or orders without notice or hearing. Proposed Section 224(b) would supplant Section 215 with respect to establishing cyber security standards. The NERC standard-setting process brings together industry and security experts to develop standards that must apply to the international, interconnected grid. Developing long-term standards that apply to the more than 1800 diverse entities that own and operate the bulk power system is a complex undertaking. Standards must apply equally to companies with thousands of employees and to those with only twenty. Additionally, the standards must not do harm. They must take into account unique component configurations and operational procedures that differ widely across the grid. Given our extensive experience in standards development, NERC firmly believes the level of expertise needed to create standards that achieve security objectives and ensure reliability can best be found within the industry itself. Given these constraints, setting these standards should not be done without notice or opportunity to be heard, especially when the consequence of noncompliance can be significant penalties.

Sections 224(b) and 224(c) also create potentially competing emergency authorities in both the Secretary of Energy and FERC, since FERC may issue an order without notice and hearing, and there is no requirement that the Commission coordinate with the Secretary of Energy or with other potentially affected nations.

NERC believes the highest priority gap in the nation's cyber security protection is the lack of emergency authority, and proposed Section 224(c) addresses that gap.

CONCLUSION

NERC, the electric industry, and the governments of North America share a mutual goal of ensuring threats to the reliability of the bulk power system, especially

cyber security threats, are clearly understood and effectively mitigated. NERC has taken a number of actions to protect the bulk power system against cyber security threats and NERC will continue its work with industry stakeholders to do so. We believe these efforts have improved and will continue to improve the reliability and security of the bulk power system. We maintain, however, that these efforts cannot be a substitute for additional emergency authority at the federal level to address specific and imminent cyber security threats.

NERC and industry stakeholders appreciate the magnitude and priority of this issue and fully support legislative efforts to address this gap in authority as quickly as possible. Moving forward, NERC is committed to complementing Federal authority to address cyber security challenges, regardless of the form it may take. We commend this Committee for its action to date and look forward to supporting its efforts however possible.

The CHAIRMAN. Thank you very much.

Mr. Mosher.

STATEMENT OF ALLEN MOSHER, SENIOR DIRECTOR OF POLICY ANALYSIS AND RELIABILITY, AMERICAN PUBLIC POWER ASSOCIATION

Mr. MOSHER. Thank you and good morning. Chairman Bingaman, members of the committee, thank you for asking me to testify this morning. I am Allen Mosher, Director of Policy Analysis and Reliability for APPA. I am here on behalf of APPA staff. There wasn't sufficient time for me to run the Dtaff Draft by APPA membership, so I am giving you a preliminary view.

APPA is the trade association of the Nation's 2,000 State, municipal, and other publicly owned utility systems. We serve about 45 million people across the country in 49 of the 50 States.

I did have an opportunity to speak with a member at the NERC Board of Trustees meeting the other day about the draft legislation and my testimony. He very much wanted me to emphasize that if the utility industry is given reliable, credible, actionable information from the Federal Government, we will act to protect our facilities. We have a vested interest in protecting both the assets and in ensuring reliable service to our customers. Its a responsibility to customers, to our communities, and to the Nation as a whole to do that.

APPA does believe that legislation is needed, but it needs to be carefully drawn and to build upon the security, cyber security and bulk power reliability framework that is already in place. We need to improve upon the NERC standards development process. Yes, it isn't fast enough, but we do believe that we can improve upon it and make it more effective and meet many of the needs that have been identified.

We do agree that there should be specific additional legislative or statutory authorities for the Federal Government, in particular for FERC and DOE. First, we support targeted authority for FERC to issue emergency orders in response to imminent threats to the bulk power system. These directives should, however, remain in effect only until the threat subsides and until we can replace them with permanent NERC reliability standards.

We also support specific authority for the Commission to address certain vulnerabilities identified in a June 2007 NERC Advisory called AURORA. In the APPA's view, the AURORA-related vulnerabilities can and should be addressed through reliability standards, but until there are standards in place that cover it, then

FERC should have some interim authority, but limited to that advisory.

We definitely need to have better mechanisms and statutory protections for communications. There are real problems communicating on the nature of threats, both from the government down to the industry and back up from the industry to the government. There are particular problems for publicly owned entities, both Federal, State, and municipal. Because we are entities of local governments, we have public openness laws that sometimes get in the way of keeping information confidential.

Let me go on to the next point. We do have some concerns with the draft. It is potentially over-inclusive of facilities, it covers generation, transmission, and distribution. We are concerned that if you include distribution facilities within the scope of the legislation, you may actually reduce the effectiveness of the overall program. By trying to cover everything, you may actually weaken the overall program.

In section 224, B–1, FERC is given very, very broad discretion to act in the public interest to protect against a cyber attack. We think there should be some limitations on that authority. It could—in fact, in the absence of prior consultation with the industry, lead to requirements that are burdensome, very expensive, and potentially ineffective. Again, the Commission can't know all of the details on all of the different utility systems. As Rick said earlier, we have very small electric utilities in the country. I have members, utilities, that have staffs of five people. It would be impossible for them to be read into the programs and to work effectively in this construct. So, thus we need to have a limited scope initially to really have an effective program for the bulk power system.

Next, the bill gives both FERC and DOE authority to act on an emergency basis. Although one is characterized as authority to act on vulnerabilities and the other is threats, this could lead to conflicts between the actions of two Federal agencies. What we really can't afford to have in the time of crisis is two directives from two agencies that are inconsistent.

Finally we need to have really far more, far more effective measures on confidentiality. The bill raises the issue, but we need a much more comprehensive structure and we would be happy to work with the committee to work out such provisions.

Thank you.

[The prepared statement of Mr. Mosher follows:]

PREPARED STATEMENT OF ALLEN MOSHER, SENIOR DIRECTOR OF POLICY ANALYSIS AND RELIABILITY, AMERICAN PUBLIC POWER ASSOCIATION

INTRODUCTION

APPA appreciates the opportunity to provide the following testimony for the Senate Energy and Natural Resources Committee's hearing regarding the Joint Staff draft related to cyber security and critical electricity infrastructure. I am Allen Mosher, Senior Director of Policy Analysis and Reliability for APPA.

APPA represents the interests of more than 2,000 publicly-owned electric utility systems across the country, serving approximately 45 million Americans. APPA member utilities include state public power agencies and municipal electric utilities that serve some of the nation's largest cities. However, the vast majority of these publicly-owned electric utilities serve small and medium-sized communities in 49 states.

My comments concerning the electric utility industry's work on cyber security issues and the Joint Staff draft that is the subject of today's hearings are offered on behalf of APPA alone. I would be remiss, however, if I did not first discuss the broad consensus within the electric power industry in support of enhanced, albeit narrowly targeted, authorities for the Federal Energy Regulatory Commission (FERC) and the United States Department of Energy (DOE) in the area of cyber security.

The associations in our industry represent a broad variety of stakeholder interests, including investor-owned, cooperatively-owned and publicly-owned utilities, independent generators, Canadian utilities, large industrial consumers, and state-public utility commissions. For very legitimate reasons, we usually have very different views on the policy issues facing our industry. On the issue of protection of the electric bulk power system from cyber security emergencies, however, we have been working together for over a year. APPA, the Canadian Electricity Association, the Edison Electric Institute, the Electricity Consumers Resource Council, the Electric Power Supply Association, the Large Public Power Council, the National Association of Regulatory Utility Commissioners, the National Rural Electric Cooperative Association and the Transmission Access Policy Study Group all support carefully crafted and specific legislation to deal with the discrete issue of cyber security emergencies. We understand the seriousness of the issue, and the need to deal with it. At the same time, we believe that such legislation must be carefully drawn and narrow in its application, to avoid disrupting the mandatory reliability regime that Congress has already required and the electric utility industry is implementing, with FERC oversight.

Attached to my testimony is a two-page issue brief* that outlines this common perspective among the electric power trade associations in support of certain shared principles. However, I must emphasize that this testimony is provided solely on behalf of APPA. I will also address APPA's initial assessment of the Joint Staff draft, although these views are only those of APPA Staff, since we were unable to review the draft legislation with APPA's members prior to the filing of this testimony.

APPA CYBER SECURITY PRINCIPLES

APPA believes legislation regarding the cyber security of the nation's electric power system should be based on certain core principles, and take into account efforts now underway. Any legislation Congress adopts should:

(1) Continue the strong industry partnership with government agencies in the United States and Canada. On an ongoing basis, the electric power industry communicates and collaborates in the United States with the Department of Homeland Security, DOE and FERC. Similarly, in Canada, the industry deals with the various federal and provincial authorities to gain needed information about potential threats and vulnerabilities related to the bulk power system. The electric power industry also works very closely with the North American Electric Reliability Corporation (NERC) to develop mandatory reliability standards, including an array of cyber security standards, which NERC calls "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. NERC is in the process of adopting important improvements to its ESISAC alert communications software that will allow more targeted communications and provide for a more secure, reliable two-way communications pathway between NERC and industry members.

(2) Foster the current electric power industry-wide commitment to continuously monitor the bulk power system and mitigate the effects of transmission grid reliability and security incidents, large and small. All sectors of the industry are working to instill a culture of compliance with mandatory electric reliability standards enforced by the Commission within the United States. Maintaining and enhancing the cyber security of our bulk power control and communication systems is a fundamental element of this developing industry culture. The electric utility industry is unlike many other critical infrastructures in the United States, in that each utility company, whether publicly or privately owned, is interconnected with and directly affected by the operating practices of its neighboring utilities. The very fact that our own actions can adversely affect the reliable operation of our neighbors gives the industry a shared commit-

* See attachment on page 32.

ment to reliability and to mandatory reliability standards. The need to maintain and enhance cyber security, coupled with the deployment of complex digital communications networks for system control, presents a new set of potential challenges and opportunities to the industry. New efficiencies made possible by smart grid for example, also present new vectors for attack upon both new and existing system control networks that could present a risk of cascading outages. On the other hand, it may be possible to design smart grid applications that provide new ways of detecting and responding to malicious activity on the electric grid.

(3) Support continued participation in NERC's industry-based and FERC-approved standards development process which will yield mandatory CIP cyber security standards for the bulk power system that are clear, technically sound and enforceable, and which garner broad support within the industry. NERC is striving to draw from the state-of-the-art in cyber security, through consideration of the National Institute of Standards and Technology's (NIST) framework for cyber security, and to integrate that framework into NERC's existing Critical Infrastructure Protection standards. As Vice Chairman of the NERC Standards Committee, I can personally attest that both NERC, as an organization, and the industry have made a significant commitment of resources to the development of new cyber security standards. In fact we've committed some of our scarcest resources—our subject matter experts in cyber security and system operations—to the task of developing draft standards for consideration by the industry as a whole. NERC has also made important revisions to its standards development process, by putting in place policies that allow, when necessary, for the confidential and expedited or emergency development of reliability standards, including those related to cyber security.

However, there are four specific areas in which APPA would support additional statutory authorities for the federal government and in particular for FERC and DOE:

(1) Narrowly targeted authority for the FERC to issue emergency orders in response to an imminent threat to the bulk power system. If the federal government has actionable intelligence about an imminent threat to, or a newly identified vulnerability on, the bulk power system, and time does not allow for classified industry briefings and timely development of mitigation measures for a threat or vulnerability, the FERC in the United States and the appropriate corresponding authorities in Canada should be authorized to direct the electric power industry to take needed emergency actions. The electric power industry is ready, willing and able to respond to specific directives based on targeted mitigation measures that are clearly linked to the nature of the underlying threat. However, these emergency directives should only remain in effect until the threat subsides or FERC approves related NERC-developed reliability standards that establish permanent measures to address the specific vulnerability that the threat was intended to exploit. In the United States, Section 215 of the Federal Power Act (added by the Energy Policy Act of 2005) invested FERC with a significant supervisory role in bulk power system reliability. It would be duplicative and inefficient to recreate that responsibility at another agency. But at the same time, it would be highly disruptive to the process for development of mandatory and enforceable electric reliability standards set out in FPA Section 215 for the FERC to impose permanent or quasi-permanent cyber security standards that have not undergone the due process steps within the industry required by that section.

(2) Specific authority for the Commission to issue orders that address certain vulnerabilities to the bulk power system identified in the June 21, 2007 ESISAC Advisory issued by NERC, and related remote access issues. In APPA's view, the vulnerabilities identified in the so-called "Aurora Advisory" can and will be addressed through the development of new NERC cyber security standards for the bulk power system that will be posted for industry comment. These standards will be comprehensive in scope and will encompass all bulk power system asset owners, operators and users in various degrees. The standards will address the potential underlying vulnerability by securing utility assets from unauthorized remote access. Until such time as those standards are adopted, however, FERC should be authorized to direct that remedial measures be taken by United States entities subject to NERC reliability standards.

(3) Improved communications flows of timely and actionable information from government to industry, matched by enhanced responsibility for the electric power industry to share critical energy infrastructure information with government agencies on a similarly secure and confidential basis. In normal cir-

cumstances, the electric power industry can protect the reliability and security of the bulk power system without government intelligence information. However, in the limited circumstances when the industry does need government intelligence information on a particular cyber security threat or vulnerability, it is critical that such information be timely and actionable. After receiving this information, the electric power industry can then direct its expert operators and cyber security staff to take the necessary steps to secure systems and networks, ensuring the reliability and security of the bulk power system. While a number of federal agencies have roles in this communication process, APPA continues to support placing DOE in the role of the lead agency in communicating threat information to the electricity sector as well as to other sectors of the energy industry. DOE's understanding of the electric utility industry provides it with the ability to filter and translate intelligence information into a more actionable form. Moreover, because DOE does not have direct regulatory authority over the electric utility industry, it will be better situated to receive candid assessments of potential industry vulnerabilities or attempts to penetrate electric power industry assets than FERC, which is charged with enforcing industry compliance with mandatory reliability standards, with penalties of up to $1 million per day for each violation.

(4) Enhanced authority for the electric power industry—particularly public power utilities—to protect and keep critical energy infrastructure information confidential and non-public. The electric power industry and government face a variety of complex issues associated with the non-public exchange of Critical Energy Infrastructure Information (CEII) as well as gaining appropriate access to highly sensitive cyber security threat information available to government agencies. For example, NERC and FERC face conflicting statutory obligations to use open, public stakeholder processes to develop cyber security standards and to approve such standards through public notice and comment, while safeguarding from public disclosure threat and vulnerability information that may provide the rationale for certain elements of these reliability standards. Public power utilities face their own unique problems in this area. As instrumentalities of state and local governments, public power utilities are subject to state public record and open meeting laws, which make keeping a variety of information non-public more difficult. As publicly-owned entities, this is as it should be—public power utilities are committed to open government and transparency. However, in the case of CEII, transparency is not in the public interest. Just as certain federally-owned utilities may face difficulties protecting information from Freedom of Information Act (FOIA) requests, even when CEII protections are invoked, state and locally-owned utilities face the risk of state record requests for such information. The transfer of such sensitive information to a third party makes protection of CEII for public power systems even more difficult. Public power systems are currently developing possible statutory approaches to address their unique CEII concerns. APPA notes that H.R. 2165, introduced on April 29, 2009, by Rep. John Barrow (D-GA) and co-sponsored by Energy and Commerce Chairman Henry Waxman (D-CA) and Rep. Ed Markey (D-MA), contains provisions intended to address these pressing information disclosure issues. While APPA has not completed its analysis, H.R. 2165 appears to comport with many of the points I have laid out in this testimony, including the need for enhanced authority to protect CEII.

APPA STAFF COMMENTS ON JOINT STAFF DRAFT

APPA staff has also reviewed the Senate Energy and Natural Resources Committee Joint Staff draft of proposed Federal Power Act Section 224, which would authorize FERC and DOE to issue rules and orders to respond to cyber security vulnerabilities and threats to critical electric infrastructure. While we appreciate the Committee working to address this important issue, APPA does have some concerns with that draft, including the following:

Inclusion of potentially all electric utility industry assets, including distribution, is overly broad.

Sec. 224 (a)(1) defines "Critical electric infrastructure" to include distribution systems and assets that if incapacitated or destroyed would have a debilitating impact on security, national economic security, or national public health or safety. Depending on how FERC and DOE make their respective determinations in implementing the statute, virtually all electric utility infrastructure could be included within the scope of this new statutory authority. APPA believes that over-inclusion of electric utility infrastructure

would be counterproductive; by attempting to protect everything efforts to protect the truly critical and important infrastructure would be diluted. APPA therefore supports targeting new FERC and DOE authority toward urgent cyber security threats to the bulk power system, rather than the broader universe of facilities envisioned in the Committee staff draft. The Committee staff draft could expose over 1,650 additional public power distribution systems to FERC and DOE regulation, imposing very substantial regulatory and financial burdens on many small cities and towns that are disproportionate to the potential cyber security risks that these entities pose. Again, APPA believes that the effort to maintain and enhance the cyber security of the nation's critical electric utility infrastructure should focus first on the critical facilities and systems that, if not protected, could cause substantial disruption to the nation's electric utility industry.

FERC discretion appears to be broad and unfettered.

Sec. 224 (b)(1) directs FERC to issue rules and orders "as are necessary to protect critical electric infrastructure from cyber security threats." [Emphasis added.] This section imposes no real limits on the extent of FERC authority to order specific actions. As written, it appears that FERC could order the enlargement of facilities, interconnections or disconnections or any other action it deems necessary, without any obligation even to consult with the industry in advance to determine whether its proposed course of action is the most effective and cost-efficient way to address a particular threat. This section would also permit FERC to issue cyber security orders that directly replace or supplement industry-approved reliability standards, undermining one of the fundamental tenets underlying Section 215.

FERC and DOE emergency procedure authorities are potentially redundant.

Under Sec. 224 (b)(2) and (c), FERC and DOE are both granted authority to act on an emergency basis without prior notice or hearing for up to 90 days, with FERC authorized to take expedited measures to protect critical electric infrastructure from cyber security vulnerabilities and DOE authorized to take emergency actions to protect critical electric infrastructure from cyber security threats. APPA suggests that such emergency or expedited authority could be assigned to a single agency, to avoid duplication and confusion as to the respective roles of the two agencies. It is imperative that agency directives not be conflicting.

The requirements to consult with industry and to mitigate burdens before directives become effective should be stronger.

FERC's authority to issue rules or orders under Section 224 (b)(1) presumably is subject to the judicial review procedures set out in the FPA, as well the Administrative Procedures Act (although these points should be clarified). DOE and FERC authorities to issue emergency orders under sections (b)(2) and (c) are subject to a 90 day sunset in Sec. (d) unless FERC "gives interested persons an opportunity to submit written data, views, or arguments. . ." Unfortunately, there is no requirement for FERC and DOE to consult with the industry in advance, even as time permits, regarding the nature of the threat or vulnerability, or to take into account the industry's views on the most efficient way in which to address the threat and/or methods for reducing the associated burden on the industry. Moreover, the filing of a request for rehearing or petition for review would not stay the effectiveness of the directive. Compliance with a potentially flawed directive would therefore be both mandatory and subject to financial penalties under FPA Section 316A (EPAct Sec. 1284).

Draft Sec. 224(f) does not fully address confidentiality issues, including the need for processes governing non-public communications between FERC/DOE and the industry, and the particular confidentiality issues faced by public power utilities.

My understanding is that the Critical Infrastructure Information Act processes referenced in Sec. 224 (a)(3) and (f) protect only voluntary disclosures by non-governmental entities to government agencies. As discussed above, a variety of other communications may need additional safeguards. As noted previously, H.R. 2165 contains provisions that deal with these confidentiality concerns in a more comprehensive and effective manner.

Thank you for the opportunity to present APPA's views on the important cyber security issues facing the electric utility industry. We look forward to continuing to work with the Committee on this important issue and we are available to provide any further assistance.

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, Senator Murkowski, other members of the committee. My name is David Owens and I am the Executive Vice President for Business Operations for the Edison Electric Institute. I certainly do appreciate this opportunity to be with you today.

I am accompanied today by Steve Naumann, who is the Vice President of Wholesale Market Development for the Exelon Corporation. Steve also serves as the chair of the Member Representatives Committee in the North American Electric Liability Corporation. So, he has extensive technical background and a good understanding of the NERC processes. I brought him in case you ask me some hard questions, so I'll turn around and say, Steve, help me out.

But let me get into just the points that I'd like to make. I'd like to really focus on three areas morning. I would like to first say that I believe that the success of public and private partnerships in recognizing and addressing cyber threats and vulnerabilities are very critical. I also believe that there is a need to avoid unintended consequences when implementing cyber security remedies. Finally, I would like to make a couple of comments about the joint draft proposal.

But let me start out and really piggyback something that Allen Mosher said earlier and that is that we take the issue of cyber security very, very seriously in our industry. Not just as utility owners and operators, but all aspects of the industry. We take it very seriously.

We also recognize, however, that our cyber adversaries are becoming much more sophisticated and so that compels that the private sector work more closely with the government in coordinating information from and to the government. So, we see that we have a significant commitment to work very closely with the government, to get a good understanding of the possibility of cyber threats and vulnerabilities.

We recognize that we have important roles and the government has important roles. We believe that both the public and private sectors, we need to have our regimes very clearly defined. We recognize that our roles are complementary and our responsibilities may be complementary, but we certainly do believe that there needs to be substantial cooperation between government agencies and utilities.

We also believe very passionately that grid security, in order to provide gridsecurity, that the manufacturers of critical components of our systems, they also need to come under some very high standards. They need to demonstrate that they are adequately fulfilling

their security responsibilities by adopting good security practices as well. Now, if our suppliers are building security into their products and providing mitigation technical assistance when new vulnerabilities arise, it permits us to operate our systems in a much more secure and reliable fashion.

We also recognize, as Pat Hoffman indicated, that there are additional potential cyber vulnerabilities as we begin to digitize our systems. As we begin to go to Smart Grid technologies, we recognize that we open ourselves up for other vulnerabilities. We believe that it is very imperative that the industry work closely with the vendors and manufacturers to ensure that they understand that cyber security is essential, so that they have cyber security protection and that they are incorporating in the devices as much as possible.

To that end, we certainly do support the process currently underway at the National Institute of Standards and Technology to develop a framework of standards that will become the foundation of a secure, interoperable Smart Grid.

Now, we are also encouraging the development of a security certification program. Let me describe that. We call it kind of Good Housekeeping seal of approval, if you will, through which Smart Grid components and systems could undergo rigorous independent testing and receive a certification that security tests have been passed. If we are using new devices and we're moving to the Smart Grid, we believe that those devices really need to be able to pass through a very rigorous screen.

I mentioned earlier the need for cooperation between the government and industry and EI members are working very closely with government partners, the national labs, the FBI, the DHS, DOE, the Office of the Director of National Intelligence and even FERC in many proactive processes to enhance cyber security. We believe that this careful consultation with utilities helps ensure that government intervention in protecting the grid from a cyber attack does not have unintended consequences.

That is because, as you know, the grid is a very complex machine. Certain measures which might prevent a particular type of cyber attack could themselves have adverse consequences on the safety and reliability of the electric grid.

So we believe, for this reason, any new legislation giving FERC or the Department of Energy additional statutory authority should be limited to emergency situations where there is significant declared national security or public welfare concerns and should provide ongoing consultation with industry experts as much as possible.

Now, we applaud the committee and the chair for the herculean efforts in the adoption of mandatory reliability standards. As was indicated earlier by Rick Sergel, there is a very deliberative process that we go through within the NERC framework and the adoption of standards. We recognize that that NERC process really is not suited for developing standards that are designed to address emergencies, where we require immediate mandatory action with the confidential handling of information.

But it is also important to recognize, as I believe, that the vast majority of cyber issues do not rise to the level of national security.

As such, we believe very strongly that the legislation should be focused narrowly on addressing a potential set of threats that legitimately merit special Federal emergency authority.

I will go back to a major theme and that is promoting clearly defined roles and responsibilities as well as ongoing consultation sharing of information between the government and the private sector, in our opinion, is the best approach to improve cyber security. EI and its member companies, we remain fully committed to working with the committee, working with the various government agencies.

I appreciate this opportunity to appear before you today and 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 am accompanied by Steve Naumann, Vice President for Wholesale Market Development for Exelon Corporation. Steve also serves as Chairman of the Member Representatives Committee of the North American Electric Reliability Corporation (NERC), and in his various roles he has more familiarity with the technical and operational aspects of cyber security issues related to the electric grid, as well as industry processes in place at NERC. We appreciate your invitation to appear today and the opportunity to testify about cyber security and critical electric infrastructure.

My testimony focuses on the nature of cyber security threats to the bulk electric power system, the efforts of electric utilities to respond to those threats, and the joint staff draft on critical electric infrastructure. I want to reassure the Committee that EEI's member companies and other owners, operators, and users of the bulk power system take cyber security very seriously. Our companies deal with cyber security issues every day as one of many important aspects of grid reliability. Utilities have many processes and programs in place to protect their cyber infrastructure and mitigate the risks that cyber intrusions pose to reliable operations of their systems.

Information about cyber security vulnerabilities and attempts to exploit those vulnerabilities is shared with electric industry owners, users, and operators through a number of channels every day. Federal agencies that communicate this information to the private sector, such as the United States Computer Emergency Readiness Team (US-CERT), as well as cyber security hardware and software vendors, classify vulnerabilities in terms of the generalized risk to systems. Factors such as the seriousness of consequences of a successful attack, the sophistication required to conduct the attack, and how widely used the potentially affected assets are within an industry are used to rank vulnerabilities as "high", "medium", or "low" risk.

Both the federal government and electric utilities have distinct realms of responsibility and expertise in protecting the bulk power system from cyber attack. As cyber security threats continue to evolve and our cyber adversaries become more sophisticated, the private sector would welcome even more coordination with, and information from, government agencies with national security responsibilities that have the best access to intelligence concerning the nature of threats to electric utility systems. Electric utilities are experienced and knowledgeable about how to provide reliable electric service at a reasonable cost to their customers, and they understand how their complex systems operate. Electric utilities are in a unique position to understand the consequences of a potential malicious act as well as proposed actions to prevent such an exploitation. 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.

As the industry relies increasingly on digital electronic devices and communications to optimize our systems and enhance reliability, cyber security will remain a constant challenge. Effective cyber security will continue to require a strong part-

nership among utilities, the federal government, and the suppliers of critical electric grid systems and components. Our companies believe they are up to their part of this task, building on our industry's historical and deep-rooted commitment to maintaining system reliability.

EEI member companies are addressing the risks they know about through a "defense-in-depth" strategy while appropriately balancing considerations of potential consequences. This defense-in-depth strategy includes preventive, monitoring and detective measures to ensure the security of our systems. For example, they perform penetration tests where a contractor attempts to find and exploit vulnerabilities. The results of these regular penetration tests inform companies about whether their preventive strategies are working so that they can enhance their protection as technologies and capabilities evolve. Penetration testing also allows them to practice and enhance their monitoring capabilities.

EEI members are also working with government partners—the national laboratories, the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), Department of Energy (DOE), and the Office of the Director of National Intelligence (ODNI)—in many proactive programs to enhance the cybersecurity of the electric grid. For example, industry participants worked with DOE to develop a strategic roadmap to identify and prioritize projects to enhance the security of electric industry control systems.

Obviously, the scope of the damages that could result from a cyber security threat depends on the details of any particular incident. A carefully planned cyber attack could potentially have serious consequences. In considering the scope of damages that any particular cyber security threat might inflict, utilities must also consider the potential consequences caused by any measures taken to prevent against cyber attack. Certain measures that might prevent a particular type of cyber attack could themselves have adverse impacts to safe and reliable utility operations and service to electricity customers. Examples might include slower responses during emergency operations, longer times for restoration of outages and disruption of business operations dependent on Internet access. That is why each situation requires careful consultation with utilities to ensure that a measure aimed at protecting the grid from a malicious cyber attack does not instead cause other unintended and harmful consequences.

Furthermore, every utility operates different equipment in different environments, making it difficult to offer generalizations about the impacts to the bulk power system or costs and time required to mitigate any particular threat or vulnerability. This complexity underscores the importance of consultation with owners, users, and operators to ensure that any mitigation that may be required appropriately considers these factors to ensure an efficient and effective outcome.

For the foregoing reasons, any new legislation giving the Federal Energy Regulatory Commission (FERC) or DOE additional statutory authority should be limited to true emergency situations where there is a significant declared national security or public welfare concern. In such an emergency, it is imperative that the government can provide appropriate entities clear direction about actions to be taken, and assurance that those actions will not have significant adverse consequences to utility operations or assets, while at the same time avoiding any possible confusion caused by potential conflicts or overlap with existing regulatory requirements.

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.

It is equally critical that cyber security solutions be incorporated into the architecture being developed for smart grid solutions, so that the great benefits new smart grid technologies will provide are implemented in a secure fashion. With smart grid solutions in the early stages of development, opportunities exist to ensure this vision is fulfilled. EEI supports the process currently underway at the National Institute of Standards and Technology (NIST) to develop a framework of standards that will become the foundation of a secure, interoperable smart grid. EEI is encouraging the

development of a security certification program, through which smart grid components and systems could undergo independent testing and receive a certification that security tests had been passed. Such a program would help utilities differentiate among different vendor solutions to select those providing appropriate cyber security.

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 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. 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, and 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 now 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, it is important to note that 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 extremely 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 joint staff draft provides DOE and FERC with parallel authorities to address cyber security threats and vulnerabilities, respectively. The joint staff 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.

Federal legislation also should require that federal emergency cyber security orders end when the emergency is past or NERC has developed and FERC has approved a mandatory standard that handles the situation. The joint staff draft provides a 90-day "sunset" for emergency actions, unless FERC affirms or amends a rule or order after receiving comments.

Any cyber security legislation should promote consultation with industry stakeholders and owner-operators of the bulk power system on remediation measures. The complexities of keeping a large, interconnected system running safely cannot be understated. Consultation is critical to improving cyber security while maintaining safe and reliable utility operations. To the extent practicable, a basic premise of existing law—involvement of industry experts to develop mitigation measures—should be replicated for imminent cyber security threats. Cyber security legislation should provide reasonable opportunity for important industry consultation, without mandating a consultation that could delay implementation of mitigation in an urgent situation.

The consultation provisions of the joint staff draft are focused mostly on after-the-fact consultation with owners, users and operators. Without stronger requirements for prior consultation where possible under the circumstances, it is more likely that federally-ordered actions, developed under time pressure and without technical input from affected entities, could cause unintended adverse consequences to electric reliability.

It is also important to note that FERC has jurisdiction under FPA section 215 over owners, users, and operators of the bulk power system, the electric reliability organization (i.e., NERC), and regional reliability entities. The scope of this authority is relatively broad, including facilities and control systems that operate interconnected electric transmission networks and generation needed to maintain transmission reliability. However, the joint staff draft appears to represent a further broadening of federal regulatory authority that would extend to local distribution systems, which historically under the FPA has been reserved for the jurisdiction of state regulatory commissions.

CONCLUSION

While many cyber security issues are already being 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.

Any new authority should be complementary to existing authorities under Section 215 of the Federal Power Act, which rely on industry expertise as the foundation for developing reliability standards. Any new authority should also be narrowly tailored to deal with real emergencies; overly broad authority would undermine the collaborative framework that is needed to further enhance security.

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 representation of industry stakeholder associations represented on the joint statement on cyber security attached at the end of my testimony.

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

ATTACHMENT.—THE NORTH AMERICAN ELECTRIC POWER INDUSTRY'S TOP PRIORITY IS A RELIABLE AND SECURE BULK POWER SYSTEM

The stakeholders of the electric power industry continue to work closely and in partnership with governmental authorities at the federal, state/provincial and local levels in both the United States and Canada in order to maintain and improve upon the high level of reliability consumers expect. Cyber security is an important element of bulk power system reliability that the electric power industry takes very seriously.

Electric Power Industry in Strong Partnership with Government

The electric power industry works closely with various government agencies on bulk power system security. On an ongoing basis, we communicate and collaborate in the United States with the Department of Homeland Security, the Department of Energy, and the Federal Energy Regulatory Commission (FERC), and in Canada with the various federal and provincial authorities to gain needed information about potential threats and vulnerabilities related to the bulk power system. The electric power industry also works very closely with the North American Electric Reliability Corporation (NERC) to develop mandatory reliability standards, including cyber security standards. In addition, NERC has an "alert and advisory" procedure that provides the electric power industry with timely and actionable information to assure the continued reliability and security of the bulk power system.

The Electric Power Industry Continuously Monitors and Acts Quickly to Ensure Bulk Power System Reliability and Security

Every day, the electric power industry continuously monitors the bulk power system and mitigates the effects of transmission grid incidents—large and small. Consumers and government are rarely aware of these incidents because of the sector's advance planning and coordination activities which reflect the quick and often seamless response the sector takes to address reliability and security events. This response includes prevention and response/recovery strategies—both are equally important. The industry's strong track record on reliability and security continues as we work diligently to adhere to mandatory NERC reliability standards, which are approved by FERC, including standards that address cyber security.

NERC Flexible Standards Approval Processes Meet Majority of Grid Challenges

NERC's industry-based and FERC-approved standards development process yields mandatory standards for the bulk power system that are clear, technically sound and enforceable, yet garner broad support within the industry. NERC is striving to draw from the state-of-the-art in cyber-security, through consideration of the National Institute of Standards and Technology (NIST) framework for cyber-security, and to integrate that framework into NERC's existing Critical Infrastructure Protection standards. NERC has also made important revisions to its standards development process by putting in place policies that allow, when necessary, for the confidential and expedient development of standards, including those related to cyber and physical security.

Emergency Cyber Situations Require an Expeditious and Efficient Approach

If the federal government has actionable intelligence about an imminent threat to the bulk power system, the electric power industry is ready, willing and able to respond. We understand it may be necessary for government authorities to issue an order, which could require certain actions to be taken by the electric power industry. In these limited circumstances, when time does not allow for classified industry briefings and development of mitigation measures for a threat or vulnerability, FERC in the United States and the appropriate corresponding authorities in Canada should be the government agencies that direct the electric power industry on the needed emergency actions. These actions should only remain in effect until the threat subsides or upon FERC approval of related NERC reliability standards. In the United States, Section 215 of the Federal Power Act (Energy Policy Act of 2005) invested FERC with a significant role in bulk power system reliability, and it would be duplicative and inefficient to recreate that responsibility at another agency. As FERC, NERC and the electric power industry relationships move forward and mature in the area of reliability and security, any disruption of this would be counterproductive.

Improved Electric Power Industry-Government Partnership with Better Information Flow

In nearly all situations the electric power industry can protect the reliability and security of the bulk power system without government intelligence information. However, in the limited circumstances when the industry does need government intelligence information on a particular threat or vulnerability, it is critical that such information is timely and actionable. After receiving this information, the electric power industry can then direct its expert operators and cyber security staff to make the needed adjustments to systems and networks to ensure the reliability and security of the bulk power system. The electric power industry is fully committed to taking the needed steps to maintain and improve bulk power system reliability and security, and stands ready to work with Congress, FERC, other government agencies and NERC on these critical issues.

SUPPORTING ASSOCIATIONS AND CONTACTS

American Public Power Association, Joy Ditto, jditto@appanet.org

Canadian Electricity Association, Bonnie Suchman, bonnie.suchman@troutmansanders.com

Edison Electric Institute, Scott Aaronson, saaronson@eei.org

Electric Power Supply Association, Con Lass, Class@epsa.org

Electricity Consumers Resource Council, John Anderson, janderson@elcon.org

Large Public Power Council, Jessica Matlock, jdmatlock@snopud.com

National Association of Regulatory Utility Commissioners, Charles Gray, cgray@naruc.org

National Rural Electric Cooperative Association, Laura M. Schepis, laura.schepis@nreca.coop

Transmission Access Policy Study Group, Deborah Sliz, dsliz@morganmeguire.com

The CHAIRMAN. Thank you all for your excellent testimony. Let me just ask a few questions and then defer to Senator Murkowski.

Mr. Mosher, you point out, and I think several of the other witnesses did as well, that the draft we have circulated here has both FERC and the Department of Energy with new authority to act on an emergency basis. You say that you think this could be confusing and that APPA suggests that such emergency or expedited authority be assigned to a single agency. Which of the two?

Mr. MOSHER. My recommendation is that the emergency authority to issue orders should be assigned to the FERC and that DOE should be given the lead role in the R&D and communications process.

It's important, I think, to separate regulatory responsibilities and penalties for enforcement for failure to comply with government regulations, put that one agency and then put the R&D, let's stretch the frontier responsibility, in another organization. I think that DOE is very well situated. I think we have immense opportunities to improve our communications to get information from the Federal Government to the industry, make it actionable, and I would hate to have a conflict of interest there.

The CHAIRMAN. Mr. McClelland, do you agree with that way of fixing the problem?

Mr. MCCLELLAND. If you could bear with me just for a moment, I brought along a statistic, if I can find my statistic. If I can't, I can almost recall it from memory.

I'd rather not comment on the capabilities of the Department of Energy, but I would like to comment on the Commission's capabilities.

The Commission is a regulator and it deals with industry. Last year for instance, the Commission issued almost 9,000 orders to the affected entities, mostly to electric utilities. We had over 400, close to 500, re-hearings. So we have a process by which we can issue an order and then we can hold a hearing to hear objections and come to a reasonable decision. We initiated approximately 50 enforcement cases and settled, or ended, 22 enforcement cases.

So the commission is well-situated as a regulatory authority to make certain that measures, if you will, emergency measures that may be applied get implemented. There is a hearing and appeals process and then there is also an enforcement arm for folks that may not be so inclined to follow the Commission's directives.

The CHAIRMAN. All right. So, you think giving the Commission authority to act in the face of immediate threats is consistent with the authority they currently have, is that what I'm understanding?

Mr. MCCLELLAND. It is authority—it's consistent with implementation. The Commission has maintained all along that we are not an intelligence or security organization. We work very closely with the Department of Energy, we work closely with Homeland Security, the Central Intelligence Agency, the Department of Defense, Nuclear Regulatory Commission, on intelligence matters.

Many of our folks, in my particular office, we're mostly experienced electrical engineers from industry. So we use that intelligence, we draw upon that intelligence. We have top-secret and SCI clearances. We use that intelligence and coordinate very closely with the agencies to subsequently work with industry to try to address the vulnerabilities.

The CHAIRMAN. Let me ask you about one other point you made in your testimony. This might be something of interest to Senator Murkowski.

You say, "Finally, Congress should be aware"—this is on page 16 of your testimony, "should be aware of the fact that if additional reliability authority is limited to the areas within the Commission's jurisdiction under section 215 of the FPA, it would exclude protection against reliability threats in Alaska and Hawaii and possibly the territories, including any Federal installations located therein." You mentioned New York City, as I understood it. Could you elaborate on that?

Mr. MCCLELLAND. Yes. Would you like the elaboration just to the cities or——

The CHAIRMAN. Elaboration on all of it, please.

Mr. MCCLELLAND. The Defense Science Board, the Energy Task Force, issued a report. It was entitled, "More Fight—Less Fuel" and it was February 2008. One of the primary findings, they didn't intend to arrive at this conclusion, but they arrived at two primary conclusions. The second conclusion, which is the one that they had not intended to reach, was that the military's critical missions are overly dependent upon the commercial power grid. The commercial power grid, in many cases, the military installations do not have sufficient back up, other than for a few hours on base for selected facilities.

That would speak very heavily—and there is also a classified annex which we could not go into in an open forum, but the classified annex named specific facilities that would be at risk.

What we wanted to make certain of was that if Congress chose the definition of, Bulk Power System under the Federal Power Act, it would do so with a complete understanding that Alaska, Hawaii, perhaps the territories, would not be included. So we couldn't assure that mandatory actions would be taken, to protect and to implement measures to protect the cyber security of those systems.

In addition, the Federal Power Act allows some discretion in the definition of bulk power system. One of the regions in the Northeast has chose to define bulk power system to largely exclude all facilities below 230,000 volts. In that particular case, and they have that discretion, subject to the Commission's review, that the process will take some time to sort through. It could take years to

sort through. That discretion essentially opts out all of New York City.

If other entities or other regions exercise that same definition, then major population areas would be excluded from cyber security protection that the Commission might employ under that definition under the Federal Power Act.

The CHAIRMAN. So, you're suggesting that we clarify what the definition needs to be under the Federal Power Act to deal with that problem and we also clarify that, if there is an additional emergency authority given to FERC, that it not be restricted just to the section 215.

Mr. MCCLELLAND. No. I'm sorry, I probably wasn't clear. We're going to keep working at section 215 definition of bulk power system. The Commission does have an ability to initiate proceedings and to clarify and issue directives on the definition of bulk power system. It's just a time-consuming process.

However, in a matter that affects national security, where timely action and targeted action is critical, for instance to the success of the military missions of the Department of Defense, that definition is not acceptable. What we have asked this committee to consider is that it not use that definition of bulk power system and initiate a separate definition that would clearly delineate where the Commission's authorities were under these emergency actions.

The CHAIRMAN. OK. Let me defer to Senator Murkowski for questions.

Senator MURKOWSKI. Mr. Chairman, I appreciate you bringing up both aspects. Certainly, the clarification on the Alaska, Hawaii, and territories issue, but also to better understand that, inadvertently perhaps, through our definition, we could be laying vulnerable some of the larger cities, whether it be Washington DC or New York.

Mr. OWENS. Senator, may I just—if I might.

Senator MURKOWSKI. Yes, Mr. Owens.

Mr. OWENS. I don't necessarily agree with Mr. McClelland's explanation. Let me see if I understand whether there is a gap here in regulation.

When he was describing the city of New York, I believe that he's describing local distribution issues, which I believe are fairly handled by the companies and the State agencies. I don't see a gap in their ability to respond to emergency situations. They understand those systems extremely well. They work very closely with the utility systems. They have a process where the government and the industry clearly understand their respective roles.

I don't believe there's any evidence to indicate that there has been a failure of those agencies or those utilities to be responsive to national threat. I would go back to 9/11 to just suggest that you, where I believe that we all applauded the efforts of the city of New York.

So, I don't necessarily agree with Mr. McClelland that we need to extend FERC's jurisdiction all the way down to the distribution level.

Senator MURKOWSKI. I want to make sure that I clearly understand this discussion because I think it is very, very important.

Now, what you're suggesting, Mr. Owens, is that, through the local distribution system, it has to be handled, and we don't need to worry about it.

Mr. OWENS. That's correct.

Senator MURKOWSKI. As I understood, what we are attempting to do through this legislation, is to allow for that authority to the FERC, if that vulnerability is present.

But you're suggesting, Mr. McClelland, if we limit it to the bulk power system, then we will not have the ability for the FERC to intervene. Is that correct?

Mr. MCCLELLAND. Yes. I guess I would like to clarify. I'm not certain that I've made my point clear.

Downtown New York City is served by a network of 138,000 volt facilities. If it's Congress' expectation that a population center like downtown New York City would be covered under an emergency provision like this, in other words that the Commission would be able to implement mitigation measures that would protect against cyber security threats and vulnerability and New York City would be covered, then that would not occur under the current definition of bulk power system in the Northeast.

Senator MURKOWSKI. Under the definition currently included in this legislation or the definition that we are currently operating under?

Mr. MCCLELLAND. The definition that we are currently operating under in section 215 of the Federal Power Act.

So, my point was to make certain that if the committee chose to exercise or to use the definition of bulk power system, as it's used in section 215, it is subject to the interpretation and application of the regional entities. In this particular case, the regional entity has excluded the network, the 138,000 volt network, that serves downtown New York City and other major facilities such, I believe there are some nuclear power plants that are also excluded from regulation, interconnections with those nuclear power plants.

So I think it's an important distinction to make.

Senator MURKOWSKI. Mr. Sergel.

Mr. SERGEL. Thank you, Senator Murkowski. If we start, I think, from section 215 that was put in place, perhaps that will make it easier.

The Congress did just a fabulous job there, and I really believe that, in defining the bulk power system as the users and owners and operators of the bulk power system and left it at that.

It has been the task of NERC, working with the Federal Energy Regulatory Commission, to determine what precisely is meant by the bulk power system. It is not defined, per se, nor should it have been. But the law goes on to particularly exclude distribution facilities. So, it's users and owners of the bulk power system and the law specifically excludes distribution.

What Mr. McClelland is saying is that, from time to time, we find ourselves where that is problematic. What a surprise that we find that it is problematic with respect to New York City, where the number of distribution facilities are so significant and the level, and sort of the voltage level, at which they conduct business at distribution is so high. So, as a consequence, it is a particular example of where it is a challenge to determine. It does not mean that it

is per se excluded under that definition. We continue to work on that.

Senator MURKOWSKI. I am going to move on because my time has expired. I don't know whether we've clarified the issue or further muddied it, but it sounds like we do need to work on this just a little bit more.

Senator SHAHEEN.

Senator SHAHEEN. I actually would like to switch topics, since I'm not any clearer on the answer to the previous question.

I want to talk a little bit about standards because most of you mentioned those in your remarks and this issue of adequate standards as we are looking to change our energy foundation in this country has come up time and time again.

So, I guess my first question to you, Mr. McClelland, is you've stated in your testimony that the Department of Energy views—actually I guess maybe I should direct this to Ms. Hoffman. The Department of Energy views the development of interoperability standards for Smart Grid technologies that include cyber security protections as a key milestone. How close are we to achieving that milestone and what kind of progress has been made and what more do we need to do in order to get there?

Ms. HOFFMAN. The National Institute of Standards and Technologies convened a workshop on April 28th and 29th to look at interoperability standards. One of the domains that was discussed was cyber security standards. NIST will hold another workshop May 19th and 20th to continue that discussion of standards.

So, the standards process is moving as quickly as possible. In the meantime, the Department of Energy has been working with utility vendors to look at procurement strategies so that, as utilities purchase Smart Grid technologies, they will have current strategies to define what some of those cyber security requirements should be in the interim, until the standards are developed.

Senator SHAHEEN. Would anybody else like to address where you think we are? Mr. Owens, you mentioned standards in your testimony as well.

Mr. OWENS. We are working very closely with Department of Energy. In fact, I would even suggest that there's going to be an important meeting on May the 18th, where we are going to talk about some of the NIST standards and how we can move forward in interoperability and we're very much in support of the direction that has been carved out.

Senator SHAHEEN. Were you suggesting that there be independent testing, separate from NIST, and how would you envision that operating?

Mr. OWENS. Yes. NIST is really complementary. When I spoke to the independent testing of the various components that would be comprising the Smart Grid, I was really speaking to the fact that, in the absence of the NIST interoperability standards right now, because the utility systems are beginning to move aggressively toward Smart Grid, that we have a way that we can verify that the technologies, the devices that are being installed in our systems, are really cyber secure. That they've gone through some independent testing, that we have a set of standards that they have to meet. So that, when we integrate them into the grid, we have a

comfort level that those facilities will not pose additional cyber vulnerabilities.

Senator SHAHEEN. So, again, how do you envision that kind of independent testing? Would there be standards that the manufacturer would have to meet?

Mr. OWENS. It would be a set of standards that would be developed and the manufacturers would be held to those set of standards. There would be an independent tester that would make sure that those component devices are consistent with the standards.

If they're not consistent with the standards, obviously the utility would say we don't want to install that piece of equipment into our overall system because we're creating a potential cyber vulnerability because it hasn't met the test.

So, it would be like a Good Housekeeping, Good Housekeeping seal of approval. All vendors would have to comply. That is actually what NIST is trying to do and this is complementary to what NIST does, but recognizing that many of our systems are already beginning to put in Smart meters and other elements to the Smart Grid. We're suggesting that we try to do something right away to make sure that there is consistency and that we are not subjecting our system to cyber vulnerabilities.

Senator SHAHEEN. Do you have a proposal for who should do that independent testing, who should be responsible for it?

Mr. OWENS. No, I do not.

Senator SHAHEEN. Anyone else?

Ms. HOFFMAN. I think it's a great opportunity for the market to develop capability in the testing and the verification.

Mr. OWENS. I would agree with that response.

Senator SHAHEEN. Thank you.

Senator MURKOWSKI. Senator Corker.

Senator CORKER. Thank you very much and thank all of you for your testimony.

Mr. McClelland, I think the Chairman asked you about whether you should or should not have the ultimate singular authority to take actions on an emergency or expedited basis. It was a pretty long answer and I think you were saying yes, but I'd like yes/no answer.

Mr. MCCLELLAND. The Commission has requested that authority, yes.

Senator CORKER. So, the answer is yes.

I noticed, Ms. Hoffman, in your opening testimony that Department of Energy is taking no position on this legislation which, by the way, I find to be kind of odd, since this is sort of in your wheelhouse. I don't know whether it's just due to lack of staffing right now or what, but in the event the legislation was changed so that FERC had solely that responsibility, would Department of Energy wish to weigh-in on the legislation at that time or does it agree with that proposition?

Ms. HOFFMAN. You're correct, Senator. The Department does not have a position on the legislation at this time. However, with all emergencies within the Federal Government, coordination and consultation are very critical in making sure that everyone is on the same page with actions and responses.

Senator CORKER. But consultation is interesting and we like that too, I'm sure, but at the end of the day, are you agreeing with the proposition that FERC should have, in an emergency you can't have two or three folks, I assume, as mentioned by others, issuing conflicting direction. You are agreeing then, by lack of weighing-in, that FERC should have this responsibility?

Ms. HOFFMAN. The Department does not have a position at this time. I know the Secretary is committed to working with the Administration on the goals and responsibilities, including determining who should have that authority.

Senator CORKER. But this legislation is going to determine that authority. So, let me just, as a follow-up, could you get the Secretary to tell us, yes/no, whether FERC should have this responsibility by itself?

I do think it's problematic, when we're looking at emergency issues, to have two organizations involved that could issue conflicting direction. Could you get the Secretary to tell us yes/no, whether it ought to be FERC or DOE? I think most of us would probably be uncomfortable with both.

Ms. HOFFMAN. Sir, I can take the question for the record.

[The information follows:]

Senator Corker, 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.

The authority to determine whether an emergency exists under section 202(c) of the FPA (16 U.S.C. §824a(c)) is a secretarial authority which may be invoked by the Secretary of Energy upon the Secretary's own motion or upon complaint. It is DOE's position that the extraordinary authority to direct immediate emergency actions to respond to and protect against particular immediate cyber risks, whether they are identified as imminent threats or vulnerabilities, should be vested in the Department of Energy. For several reasons, we believe this emergency authority should be exercised by DOE, rather than by an independent regulatory agency such as FERC.

Since 1977, when the Department of Energy Organization Act created both DOE and FERC, the FPA section 202 emergency authority has been vested in DOE. Throughout Administrations involving several different Presidents and both parties, the Department has used this authority judiciously but effectively to address particular situations in which such an order was necessary to help ensure reliable supplies of electric energy.

The Department has demonstrated that, when circumstances warrant, it can exercise the section 202 emergency interconnection authority very quickly. For example, on August 14, 2003, when the largest electrical blackout in the history of North America occurred, DOE exercised its section 202 authority by issuing an emergency interconnection order only hours after the blackout occurred. It was able to do so, in part, because the Secretary of Energy can issue section 202 orders unilaterally, and need not convene meetings or collect votes of other officeholders before exercising that emergency authority.

New authority to deal with cyber emergencies also could be exercised quickly and effectively by DOE. Moreover, we believe that an extraordinary authority such as this is appropriately placed in a cabinet department whose head is fully accountable to the President. Independent agencies are just that, independent, with respect to many decisions, and while that certainly is appropriate with respect to many matters, we believe the exercise of emergency authority is not one of those matters.

Finally, DOE is the agency that is most likely to develop or obtain knowledge—either on its own or as a member of the intelligence community (IC)—with respect to threats or vulnerabilities that might give rise to the need for an emergency order. DOE regularly participates with the other agencies who are members of the IC on a variety of initiatives. It makes sense to vest an authority to act on that informa-

tion with the agency that is most likely to develop or have knowledge about it, and that agency is DOE.

FERC should be authorized, after consultation with DOE, to issue expedited reliability standards under section 216 of the FPA to respond to cyber risks.

Ms. HOFFMAN. I would like to bring up emergency versus vulnerability. The legislation brings up two aspects, one of which is emergency authority with the determination that there is actually a threat out there. The vulnerability part of the language, as we read it, provides for an interim measure: if there is a vulnerability that is discovered within the electric sector, then there is action that may need to be taken on that vulnerability, if that vulnerability is determined to have a potentially significant impact to the electric sector.

So, one actually looks at a threat environment, and the other one actually looks at a vulnerability that may be discovered for which it may be prudent to take action on a near-term accelerated basis.

Senator CORKER. So, since there is a difference, are you saying that DOE should look at the vulnerability issue and FERC should command in the event of an emergency, is that what you're saying? Or are you not going to weigh-in again?

Ms. HOFFMAN. The Department does not have a position at this time.

Senator CORKER. That's interesting. I assume there's some staffing issues that maybe caused this and I certainly don't want to in any way embarrass you. If you could maybe get whoever it is that would like to weigh-in, to weigh-in on behalf of the Department at the appropriate time before we pass this out of committee, which I assume is going to be like in a week, is that correct?

Senator MURKOWSKI. I think it is scheduled for next week.

Senator CORKER. That would be helpful to everybody. We obviously want to work, as you mentioned, in cooperation.

Did you want to say something, Mr. McClelland?

Mr. MCCLELLAND. Yes. I would like to say that the draft bill does make an important distinction between the responsibilities of the Department of Energy and the FERC. The bill designates the ability to address vulnerabilities to FERC and threats to the Department of Energy.

So, in this particular draft, the Commission staff didn't necessarily see a conflict or an overlap between the Department of Energy's role and FERC's role.

Senator CORKER. The industry folks agree with that?

Mr. OWENS. We think that needs to certainly be a clear understanding of who deals with cyber threats. So, if that's the Department of Energy or FERC, as long as there's a single agency, a clearly defined authority. With respect to cyber vulnerabilities, I believe FERC already has the responsibility and they have been implementing elements of that through their standards under section 215 of the Federal Power Act.

Senator CORKER. Mr. Sergel, you mentioned that y'all were working on some of the definitional issues that, you know, New York City has been thrown out multiple times during the course of this testimony, that y'all were working on the definitional language and that's evolving.

However, since this legislation is to focus on cyber security and other kinds of things, would it be relevant for us to work out that definitional language in advance of passing this legislation or just leaving it somewhat abstract when, in essence—I guess we're trying to figure out a way to actually deal with real threats that exist. I'm just curious as to what your response might be to that.

Mr. SERGEL. We are attempting to work out the precise lines of the definition between distribution, which is excluded from section 215, and the bulk power system in which we have authority. There are, not a long list, but certainly a list of places where it's difficult, New York being the best example.

I think the question on the distribution side goes more to the necessity of the authority that you want to grant in an emergency as opposed to that.

So if, in fact, the authority of the—to act in an emergency is intended to cover everyone, and you wish to do that in this legislation, you would want to then specify who that is and it would extend, for example, to those places that are not interconnected with the United States, excluded from section 215, Alaska and Hawaii and Guam, not interconnected. So you would be extending the definition from 215.

If you just think of it, 215 is covering a portion, the largest facilities, the largest lines, but it doesn't include distribution. So, I would think you would want to say, what do you what to include. I would go from 215 and then I would decide what you were going to add. It's 215 plus.

If it was all of distribution, my own view is that all of distribution is a reach, that that is not necessary here. But then, at the same time, I understand where it should be broader than the current definition of 215. Alaska, Guam, Hawaii, potentially very large metropolitan areas like New York and Washington which—military facilities, but I would add. I would start from the definition of 215 and decide how much to add. If you decided to add all of distribution, that would be one way to do it.

Senator CORKER. Madam Chairman, is it OK if I continue to listen?

Senator MURKOWSKI. Yes, that's fine.

Senator CORKER. OK. Mr. Mosher.

Mr. MOSHER. Yes, thank you, Senator. I would suggest that the committee look and think seriously about starting in the other direction and figuring out which customers you are trying to protect and you're most concerted about.

Rather than encompassing all of distribution, if you're concerned about New York City or Washington DC or military facilities, then you need to talk—for example, starting with military, with the base, commanders there, identify their vulnerabilities an then assign authority or set up regulations that would ensure that those particular facilities are protected. That involves the relationship between the particular distributing utility and the customer.

Now, New York City and Washington DC I know are areas of particular concern. Frankly, I think that bulk power reliability standards and the authority that is contemplated for the Commission will, in fact, cause the utilities that serve those areas to adopt standards and policies and to train their personnel so that they

will have cyber protection for the entirety of the enterprise. That's the underlying part of the NIST framework, is that it is not a facility-specific program, that is NIST for cyber security.

Its about protecting your entire enterprise and making sure there is no backdoor way of attacking the system. If you do it for the entire utility, you are indirectly going to protect the distribution facilities as a part of it.

Senator CORKER. I know my time is way beyond over. Thank each of you for your testimony.

I hope that what you may consider is that, my sense is that we are going to have a markup on this very soon, is that, on the definitional issue we just discussed, but also the definitional issue of critical electric infrastructure and cyber security threat, those two terms. I would encourage each of you to submit to us some clarifications that you think might be helpful to us.

Again, Ms. Hoffman, thank you very much for being a good soldier today and hopefully somebody from the Department will respond to the questions.

Thank you all very much.

Senator MURKOWSKI. Thank you, Senator Corker. I think it is important to note that we do have this on schedule for next Wednesday for potential markup, if all goes as planned.

I think you have raised some good issues here today. It is important to try to get that input from the Department and we recognize that there is a lot happening, not the least of which is that people aren't entirely in place and perhaps might not be focused on this, but we are trying to move on it.

I might note, and it may have been already brought up by the chairman, but we are not the only committee looking at the issue of cyber security. There is legislation out there that would have FERC be consulting with Department of Homeland Security. You have also legislation coming out of the Commerce Committee where it would be the Secretary of Commerce that is providing the direction. You've got another bill that would establish an Office of National Cyber Security Adviser within the executive branch. So, it's kind of all over the board right now.

I guess I'll throw-out this question to all of you. There has been some discussion about whether or not we need a cyber security czar. Is that where you go with it, Mr. Mosher?

Mr. MOSHER. My view is that the committee ought to focus here on the particular concerns of the electric power industry and solve those as surgically as you can, because the issue of cyber security is so much bigger than the electric power industry.

The Federal Government, the executive branch, and Congress need to come to a meeting of the minds of what that Federal Government strategy is. Then you could do a comprehensive strategy, whether it entails a cyber czar in the White House with a special office there, whether the authority is assigned to NSA, or whether it is shared with DHS. Those are sort of level issues that are, frankly, much beyond our paygrade.

But we would like to see that our particular vulnerability issues and authority issues are resolved pretty quickly. We certainly are willing to work with the Congress to resolve that as quickly as we

can. We hope that we can work with you to get something that we can all agree upon as part of the comprehensive energy bill.

Senator MURKOWSKI. Mr. Sergel.

Mr. SERGEL. Thank you. I agree with Allen, but not just overall, but within the specific confines of this bill as well. That the emergency authority for cyber security is extremely important to us. We need that. It is important to complement our standards. Our standards are incomplete without that authority.

So, it is taking action on those things that we can do today to protect the bulk power system in that situation. Certainly we will work to get our definitions as precise as we can, to make that as effective—but it is to do that portion of it that is so important. There's always the broader and larger picture, but for this industry we need emergency authority granted to a single agency.

Senator MURKOWSKI. Now, that's fair and I appreciate that.

I was reading an article here that was posted in the Wall Street Journal this morning and it attracts my attention because it details a report that the air traffic data systems in Alaska were shut-down by hackers. You know, when you're a State like mine where everybody flies and you've got your air traffic control systems that have been breached, this is a real problem.

Not to suggest that it is greater than the electrical, we recognize in today's world where we are connected in many different ways, there is a level of vulnerability in our day-to-day lives that we could never have imagined a couple of decades ago. So, whether it is occurring with air traffic control or electricity or just security in general.

Let me ask a question. We did not address this in our legislation, but it's the issue of the potential costs. There has been some concern expressed with the cost of compliance, whether it's an emergency order through DOE or FERC's expedited rules, and the concern that merchant suppliers can't pass these costs on that they need to incur in order to address the cyber security threats.

Do we just consider these costs as part of doing business in today's world or should there be some kind of cost recovery mechanism included in our legislation? Because, as I said, we have not included it, but what's your position, Mr. Sergel?

Mr. SERGEL. Just two things from me and then I'll turn it over to David Owen.

First, the way standards are set under section 215 with the industry participating assures that the costs of taking an action are incorporated in the decision itself. Because it's part of the process and it's reflected there and it's very important.

The second is that 215 address the bulk power system because it is the priority, it is the one in which we're most in danger. I point to the length of time—we had an event in Florida and it was over in an hour; whereas, the August 2003 blackout, it took days to recover from that same event in many places. So, it is very important that we deal with the bulk power system, large scale, are whole orders of magnitude greater concern.

So, from the standpoint of what it costs, let the standards and processes we have today do the job and focus on the bulk power system. It is where the highest priority is. So, for costs, those would be my suggestions.

Senator MURKOWSKI. Mr. Owens

Mr. OWENS. Soon after 9/11, FERC adopted a policy because it recognized that companies wanted to secure their systems. They said, in emergency situations, they would focus on getting you cost recovery.

So, I think it's very, very appropriate for merchant generators, who don't serve retail customers and don't go before State PUC, that to the degree that we're responding to emergency standards, standards relating to cyber, to reduce cyber vulnerabilities and so forth, it is very, very appropriate that they get cost recovery. I think that is very consistent with how FERC has dealt with issues in the past.

Senator MURKOWSKI. Mr. McClelland.

Mr. MCCLELLAND. I'd like to add to that. In fact, David stole my thunder. The Commission did issue a policy statement after 9/11 that said it would prioritize cost recovery filings for security reasons, for security aspects. So, the Commission is very aware of that.

As a staff member, I can say that it seems reasonable and I would support, as a staff member, support cost recovery filings in order to comply with measures necessary to protect the bulk power system, be they cyber or be they physical.

If I could just stir the pot back up again, because it seems like it's settled down a bit too much, back to the issue as far as the definition of bulk power system. Smart Grid actually would enable a new type of attack vector. Rick has talked about the priority associated with the bulk power system, but if you could imagine many millions and millions of distribution meters being installed on the Smart Grid that have a two-way communication capability and would be interacting, perhaps, back to an ISO or some central control center, that is another path, and a substantial path, for compromise. There are several different attack vectors that can be associated with the installation of those type meters.

So, it's a complex issue. It's ever-changing.

Senator MURKOWSKI. Do we need additional Federal authority as we reckon with the complications, as we look at the Smart Grid?

Mr. MCCLELLAND. I think the committee needs to consider that aspect and I think it needs to be well-aware that, as Smart Grid is implemented, and as these devices, these formerly dumb appliances that couldn't communicate now can communicate in two directions, any time there's two-way communication, there's a chance for cyber compromise.

The current draft does go through the distribution levels, so it appears to be a mechanism by which Smart Grid could be addressed. But it would be an expansion, a significant expansion, of the Commission's authority, if the Commission were selected as a lead agency to implement these mitigation measures for the vulnerabilities.

Mr. MOSHER. If I may?

Senator MURKOWSKI. Senator Shaheen.

Mr. MOSHER. Very briefly. The Commission has no rate jurisdiction over distribution.

Mr. MCCLELLAND. That's right.

Mr. MOSHER. So, if the costs are incurred at the distribution level, then this should be something before the State public utility commissions.

Also the mechanisms for guaranteed rate recovery for independent power producers does give public power systems some heartburn. I'll leave it at that.

Senator MURKOWSKI. Senator Shaheen

Senator SHAHEEN. Thank you. I want to go back to the definition because I guess I'm a little confused by the previous exchange.

Because, as I look at the bill, it defines critical electric infrastructure and would amend the Federal Power Act and it seems to me it is a pretty comprehensive definition because it defines it as "systems and assets, whether physical or virtual, used for the generation, transmission, or distribution of electric energy affecting interstate commerce that is determined by the Commission or Secretary" however that gets resolved "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."

I mean, I guess, as I read this definition, it would address the concerns that you all were raising. Do you think that that definition is not adequate? If it were adopted in the bill.

Mr. SERGEL. The definition in the draft legislation is the broadest one possible.

Senator SHAHEEN. Right.

Mr. SERGEL. You're are absolutely correct. It does not need to be broader to increase the protections.

The current section 215 covers only the bulk power system, the largest lines and plants, and the interconnected system in the United States; therefore excluding both distribution and Guam, Alaska, Hawaii as well.

Senator SHAHEEN. Right.

Mr. SERGEL. I think NERCs position on this is that we start from the bulk power system because it is the highest priority that needs to be protected. Then additions to that definition to expand it should be carefully done, because the authority being granted here is so great.

Now, there's two different components of the draft. One component of the draft is for emergency authority and, on that, I would say——

Senator SHAHEEN. Which is the definition I just read.

Mr. SERGEL. Yes. So, as it relates to giving emergency authority on that expanded definition, we will all work to make sure that we understand how that should be done and how it should be done effectively.

For example then, when you move to the vulnerabilities language, I would be willing to say I think that definition is too broad for the vulnerabilities language because it would give the authority to order distribution, order distribution companies to take actions from the Federal Government which is not in place today.

So I think that definition is broad enough to protect for cyber security but is actually a reach too far with respect to standard setting. On emergency authority, it is logical. On standard setting, it is a reach too far.

Senator SHAHEEN. So, is everyone on the panel in agreement that, in terms of a definition for an emergency situation, that that definition is adequate? Or is there some objection from the rest of you that that's going too far?

Mr. MOSHER. It is my view that the definition goes too far on distribution, even for emergency authority. To have a regulatory program that is actually going to be effective, I can see it cratering just in the number of entities that the Commission would have to preestablish communication pathways to make it work. If it has an authority to issue an emergency order, then it presumably needs to know it's going to contact. If it has to contact all of the roughly 1,650, one thousand six hundred and fifty, municipal systems in the country that are not on the NERC compliance registry, then the FERC would have to establish who that contact person is, what clearances they have, and have the ability to execute it. Now——

Senator SHAHEEN. If there's a current emergency——

Mr. MOSHER. I'm sorry.

Senator SHAHEEN. If there is a current emergency, how does that work? I mean, right now in the absence of this kind of legislation to address cyber security, if there were an emergency effecting the municipal utilities, how would that be communicated to them?

Mr. MOSHER. Today, within the scope of NERC's authority, they're communicating primarily with the registered entities. We are working to expand their ability to communicate through the ESISAC, the Electricity Sector Information Sharing and Analysis Center, excuse me for the acronym. We will be improving it and have voluntary communications that well reach basically all municipals over time, but it is not in place yet.

We, again, are trying to prioritize getting the communications down where the risks are the greatest, which are in the larger communities.

My concern is not in the emergency authority, but it is the regulatory hooks that come with it and the effectiveness of the communication to make sure that, for example, when Joe sends out a directive, he needs to know if the other person on the other end of the line has a security clearance. I know for a fact that we can't get security clearances for all of these entities. It would just overwhelm the capability of the FBI to do, to get all of the clearances done. People change jobs and, you know, people are performing multiple functions. It just isn't going to work.

I am suggesting a more targeted approach going to defense establishments and to addressing whatever concerns you have with large cities. That could be the way of focusing, that would be my recommendation.

Senator MURKOWSKI. Mr. McClelland.

Mr. MCCLELLAND. When we meet as Federal agencies and we discuss cyber security and cyber security issues that would affect the electric utility industry, when we speak about the electric utility industry, we say they're out in the wild. The reason why we say that they're out in the wild is that they don't have information regarding the current threats and the current activities that are being propagated on the electric grid.

One thing I would like to address that Allen had said was that we needed a security clearance or would need a security clearance

to communicate with entities. Our assumption would be that if we broadcast the information out to a large number of entities, forget it. That information will be disclosed. So the advisories or the orders that we would issue, the advisories that NERC crafts and the orders that we would issue, would be carefully crafted so as not to compromise national security, but would provide clear direction.

The testimony that I gave today, the oral and written testimony, was merely intended to reflect the fact, or inform the committee, that there is a clear distinction between—there is a limitation under 215 as to how far the Commission can reach.

The Staff Draft, however, went much further and captures even distribution. That capturing in effect, or that effect, would in turn capture the Smart Grid meters, the meters that would be deployed. We didn't address the complexities associated with an agency and exercising that control. But the definition seems to, and the testimony is intended to say, that the definition is very broad. If the committee intends to move in that direction, the committee should understand that Alaska, Hawaii, the territories, and the larger urban areas should be captured, from the Commission's perspective, and that we were advising you in regard to that definition.

In other words, the definition appears to be adequate and separate from the definition of bulk power systems in 215.

Senator SHAHEEN. But that's why I'm still confused. Because, if the definition says it would cover any system that would have a debilitating impact on national security, economic security, public health or safety, why would that not then effect Alaska, Hawaii, and the territories?

Mr. MCCLELLAND. I think the question would be what was intended by the draft and how does the Federal Power Act capture Hawaii—Alaska and Hawaii and the territories.

Senator SHAHEEN. So, do you also share the concern expressed by others on the panel that this definition is too broad?

Mr. MCCLELLAND. It depends on what the intent of the committee is. If the intention or the direction of the committee is to ensure that the agencies, the Department of Energy and the Federal Energy Regulatory Commission, would have sufficient authority to be able to address cyber security threats that could affect the United States, could impact the mission of the Department of Defense, the military facilities, then no. I would say no, the definition is not too broad, if you intend to capture Alaska and Hawaii and the territories.

If, however, you intend to limit it to say, the continental United States, in just the definition of bulk power system under 215, then you should be advised that there are limitations with that definition and complexities associated with the interpretation and the administration of that definition.

That, in and of itself, if one is speaking about national security, that could render the actions ineffective. If there is disagreement about where it applies and how it applies and whether or not it goes to a downtown urban area and there is some room for interpretation or discretion, you really can't be sure that the directive you've issued will be effective to address the cyber security concerns.

Mr. OWENS. Senator, can I try to just simplify this? I think we are making it a little bit too complicated.

You asked if the definition is too broad. If you are seeking to define a national emergency and you know the components that make the electric system, the definition covers the broadest of the electric system.

But then if you're speaking to how do I define a cyber vulnerability and what is the level or the scope of authority of the Department of Energy and the Federal Energy Regulatory Commission, you are raising a different set of issues. So, we have to separate cyber threat from cyber vulnerability. In a cyber threat, you certainly do, even Allen's members want to know, that if there is a cyber threat it needs to be well-communicated to them so they can take corrective action, so we don't have widespread disruption.

So I don't think anybody has a problem with that. We need to make sure that there is a single agency that has that responsibility and we are clear and there is ongoing communication with the utility and people that have security clearances, so they can huddle together and say, here the solutions to deal with this immediate threat.

Senator SHAHEEN. OK. Can I stop you right there? Because that is not what I heard Mr. Mosher say.

Mr. OWENS. No, I just changed it a little to say——

Senator SHAHEEN. Yes, you did. Do you agree with what he just said?

Mr. MOSHER. Yes, I do. If you're talking about communication——

Mr. OWENS. Yes.

Mr. MOSHER [continuing]. Then I agree and what David was saying is we get the experts together talking to the Federal Government, experts from the industry, experts from the government, distill the threat down to something that is actionable.

Mr. OWENS. Exactly.

Mr. MOSHER. Take out, because of a need-to-know basis, take out all of the underlying threat information that should be classified, tell the entities what to do.

Mr. OWENS. Exactly.

Mr. MOSHER. That can be communicated. Now the question where we may differ is on whether there is a regulatory structure that is imposed upon this to say that if the entity that receives the information does not comply, then there will be sanctions.

Mr. OWENS. Exactly.

Mr. MOSHER. it's when you get to the sanctions that the process breaks down because the regulatory burden increases. The entities that receive this information are going to respond to it, but they're very different in their capabilities to respond to this information. They are different in the vulnerabilities that they present to the Nation. Small municipals with one stoplight aren't in the same category as PEPCO.

Mr. OWENS. That's right.

Senator MURKOWSKI. Senator Corker.

Senator CORKER. I think this hearing is coming to a close pretty soon and we've got a four page bill, OK. It's not like—it's pretty short.

I think we've found through this Q&A time that it maybe doesn't adequately address some of the definitional issues that are important to each of you that actually have to do this on a daily basis and you're asking what the intent of the committee is.

Look, I mean, we're Senators. You know, let's face it, we do not understand fully, as each of you do, and that's why you're here, exactly how this language effects you on a daily basis. I think our concern is—we're concerned about cyber security, OK? We're concerned about making sure that Americans, including those in Hawaii and Alaska, wake up and have power to do the things they need to do and that our country has the ability, through its military, to do things necessary.

So, I would suggest that the four of you, and if the DOE determines it wants to weigh-in, and I think it might, that y'all take these four pages and make it work and give us the input back. Even if it's six pages, OK, to sort of deal with this. I mean, it's evident that you guys have a wealth of knowledge that we don't, that's why you're here. I would just ask you to help us with this. Because it sounds like that we, in some ways, in trying to solve this problem and could raise more questions than answers.

So I'll conclude with this, at least my portion of it. Mr. McClelland, you mentioned that there are issues in addition to cyber security that we need to be addressing. That there are other national security threats to reliability and I'm wondering if, in this little four-pager that we have, that could be five, six, seven, eight, are there are other powers, as it relates to the reliability side, that you feel like we ought to be addressing for FERC right now?

Mr. MCCLELLAND. Is that a question now?

Senator CORKER. Yes.

Mr. MCCLELLAND. Oh, I'm sorry.

Senator CORKER. That wasn't a yes/no one, that was a——

Mr. MCCLELLAND. Oh, yes.

Senator CORKER. No, no, no. That was not a yes/no one, OK.

Mr. MCCLELLAND. Yes, there are. Our point in the oral remarks and the written testimony is that there are physical attacks that can occur on the power grid and those attacks can be just as devastating as cyber attacks.

So if Congress would entrust an agency to exercise, be able to exercise directives, not ask for voluntary measures, but exercise directives over the industry, the affected industry for cyber, our position is that it should consider, or it should also grant the agency an extraordinary ability, or ability under extraordinary circumstance, to also exercise actions against physical threats.

A good example is a bulk power system transformer. If there were some, if there were some issue, if there were some information, that would indicate that these transformers were affected, the affected agency or the agency in charge could then issue a directive to help or to give guidance to the affected industry to protect those transformers. Perhaps relocate the transformers or take other actions in order to secure those transformers for a period of time.

Senator CORKER. So, I noticed the two guys on the end sort of shrieking. So——

Mr. MCCLELLAND. Yes, I wouldn't be surprised. We all know each other.

Mr. MOSHER. There are numerous police agencies in the United States and the FERC is not among them.

Mr. MCCLELLAND. Right

Mr. MOSHER. Particularly for municipal utilities, where we have a local police department, they are frankly very good at maintaining local security. They know who isn't from the community and is lurking around the substation.

I agree with Joe that there are physical concerns security concerns. I do not think that the FERC is the appropriate agency to undertake that.

Mr. OWENS. I would agree with. I think that there are other agencies that have that responsibility. I think Joe is right that there are elements of our system that present some vulnerabilities.

He mentioned specifically transformers and we already have an industry effort underway to make sure that we can secure, if we have a disruption in our transformers, we have an inventory of transformers that can be quickly mobilized so that we can make sure that electric service is restored very quickly.

FERC has blessed that approach, but FERC is not the agency that deals with all the physical aspects of our systems. I think that there does need to be coordination. If that is what Joe is indicating, I do agree with him that there needs to be ongoing coordination between the Federal Government and the State and local agencies.

Senator CORKER. Mr. Sergel.

Mr. SERGEL. On physical security, I worry that too many agencies that are qualified will show up to help. On cyber security, I lie awake at night worrying that no one will show up. It's cyber security emergency legislation that is absolutely essential.

There are physical issues, they are real. But, again, I agree with my associates that that is not—first, it is not the priority that I have but it's also—others would be the ones who would be better suited to do that.

Mr. OWENS. Right.

Senator CORKER. Madam Ranking Chairman, I think we've had some great witnesses and I do—did I say ranking chairman? Yes. Acting chairman, acting chairman.

I do wonder if we are ready to do this next week. Either, I mean, I know it is just a short piece of work, four pages, but it seems like a very, very important issue and it seems like that these witnesses have some clarifications that could be incredibly helpful. Either they have some quick work to do and all of us just sort of sit around and think that what they do is good or maybe we ought to think about may be looking at this some more.

I know you're very concerned. I've heard you talk several times about cyber security and I know the Senator from New Hampshire is, too. I know our whole country is. I just wonder if we're adequately addressing this right now, so.

Senator MURKOWSKI. Thank you Senator Corker. I think we all share the concerns and I'm pretty certain that the folks within the White House are very keyed on this as well. Whether it's cyber security within the power grid or, as I mentioned, cyber security issues that crop up in our aspects of day-to-day life in commerce.

But the problem is is that perhaps they have not moved as quickly in determining how they are going to approach the issue of cyber security.

Again, I threw out this whole discussion about a cyber security czar. I'm not convinced it is necessarily needed, but I think it speaks to the issue that we're faced with today. There is a level of vulnerability that we have, the smarter that we get. Our ability to utilize new technologies, and Smart Grid is a perfect example of how it makes our life better and more efficient, but exposes us to a level of vulnerability if we don't build securities into our system. We've got to be on top of this in a very, very strong way. So, the issues that have been presented today, I think, have been very helpful.

I think you're right, Senator Corker, we have recognized that, as part of a Comprehensive Energy Bill, we would be foolish not to include some aspect of cyber security into an energy piece, but how we define it and who we place in charge is key and it is critical that we do our best to try to get it right.

So, I appreciate the input from the witnesses here today and the good exchange from committee members this morning.

Thank you.

[Whereupon, at 11:45 a.m., the hearing was adjourned]

APPENDIX

RESPONSES TO ADDITIONAL QUESTIONS

FEDERAL ENERGY REGULATORY COMMISSION,
Washington, DC, May 8, 2009.

Hon. JEFF BINGAMAN,
Chairman, Committee on Energy and Natural Resources, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: Thank you for the opportunity to testify before the Senate Energy and Natural Resources Committee on May 7, 2009 on cybersecurity of the nation's electric grid. Enclosed are my responses to the post-hearing questions that you and Senator Murkowski have submitted.

Also enclosed is a one-page document with edits to the Joint Staff bill on two issues addressed in my testimony. First, the edits would broaden the bill to cover not only cyber vulnerabilities and threats but also other national security vulnerabilities and threats. Second, the edits would include additional information within the scope of subsection (f), on protection of critical electric infrastructure information.

Should you need additional information, please do not hesitate to get back in touch with me.

Sincerely,

JOSEPH MCCLELLAND,
Director, Office of Electric Reliability.

[Enclosure.]

RESPONSES TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. In your view is the authority granted in the proposal sufficiently broad to allow protection against all cyber security threats and vulnerabilities? Does the provision cover Alaska, Hawaii, and distribution systems?

Answer. Yes, my view is that the draft bill provides adequate authority on each of these points. First, the draft bill allows protection of critical electric infrastructure against all cyber security threats and vulnerabilities. Second, as to Alaska and Hawaii, the draft bill covers systems and assets used to produce, transmit or deliver "electric energy affecting interstate commerce." It is Commission legal staffs view that the Commission could reasonably find that electric energy in Alaska and Hawaii affects interstate commerce. Finally, the draft bill includes systems or assets used for "generation, transmission, or distribution" (emphasis added) if they are "so vital to the United States that the[ir] incapacity or destruction ... would have a debilitating impact on national security, national economic security, or national public health or safety."

Question 2. The condition that allows a utility, under current NERC standards, to accept the risk of inaction is a little puzzling to me. Does that mean that, if a utility says that it is willing to accept liability for all the costs of a massive outage, perhaps into the hundreds of billions of dollars, it does not have to take steps to prevent that outage? Is there any requirement for indemnification or warranty that the utility would be able to bear the cost?

Answer. While the current CIP (cyber security) standards have several requirements that allow an "acceptance of risk" in lieu of mitigation, the standards do not make clear the legal liability for such acceptance of risk. For example, Requirement R3.2 in CIP-007-1 states: "The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk." The Commission's Order No. 706 required replacing the unilateral acceptance of risk with a "technical feasibility" exception mechanism that includes an independent approval. Version two of the CIP standards recently

approved by the NERC Board of Trustees deletes all uses of the "acceptance of risk" language. Version two has not yet been filed with the Commission. Depending on the time required for the version two CIP standards to be filed and approved, under the effective date provision embedded in those standards, they could be effective as early as January 1, April 1 or September 1 of 2010. (The applicable provision in the standards makes them effective on the "first day of the third calendar quarter after applicable regulatory approvals have been received.")

Question 3. How long did it take for these NERC rules to he developed, and how much longer might it take to get them amended to correct the weaknesses?

Answer. It took approximately three years for the NERC rules to be developed. The CIP standards began as the Urgent Action (UA) 1200 standard (voluntary standards), which became effective in 2003. It was intended to he temporary measures until permanent ones could be developed and agreed upon. The current CIP standards replaced the UAl200 standard on June 1, 2006, after they were approved by the NERC Board of Trustees, and were filed with the Commission on August 28, 2006. After considering public comments on the issuance of a Staff Preliminary Assessment and on a Notice of Proposed Rulemaking, the Commission approved the CIP standards on January 18, 2008, but immediately directed NERC to make substantial modifications. NERC formed a standards drafting team to address those Commission directives. That team is addressing the required modifications in phases. The first phase has been drafted and recently approved by the NERC Board of Trustees. Once it has been filed with the Commission, and if it is approved by the Commission, that version (version two) will then he mandatory and enforceable in the continental United States. Depending on the time required for the version two CIP standards to be filed and approved, under the effective date provision embedded in those standards, they could he effective as early as January 1, April 1 or September 1 of 2010. (The applicable provision in the standards makes them effective on the 'first day of the third calendar quarter after applicable regulatory approvals have been received.") The same drafting team has been working on an anticipated phase two and a phase three to address the remaining Commission directives for modifications. I do not have a good estimate of when phase two or phase three of the modifications will take effect.

Question 4. You say that NERC reported that only 29% of utilities reported owning any critical assets. Do you have an idea of how many utilities own critical assets?

Answer. As a point of clarification, NERC reported that only 29% of Generation Owners and Generation Operators reported identifying at least one critical asset. NERC also reported that approximately 63% of Transmission Owners identified critical assets. The Commission does not have any data on how many utilities own critical assets. However, NERC's Compliance Registry Matrix identifies a total of 1,555 Generator Owners (GOs) or Operators (GOPs) and 321 Transmission Owners (TOs). NERC standard CIP-002 is entitled "Cyber Security Asset Identification" and it requires these entities to develop a "risk-based assessment methodology" to use in identifying their critical assets. The entities are then to use this methodology to self-determine their critical assets and subsequently, critical cyber assets that are captured by the cybersecurity standards. In Order No. 706, the Commission directed NERC to, among other things, provide guidance on the development and application of the risk-based assessment and to implement independent reviews of the individual entity's critical asset determinations. The NERC survey described on page 6 of my written testimony is part of this still-ongoing effort.

Question 5. We have tried not to eliminate the NERC standards setting process in our bill. The intent is that FERC establish standards for vulnerabilities as quickly as possible, that could then be superseded by NERC standards when such are developed that the Commission finds acceptable under the statute. Is this your reading of it as well?

Answer. I agree that the bill does not eliminate the NERC standards setting process. The Commission would have the ability to move quickly and effectively to address vulnerabilities under the new provision, followed by standards development activities by NERC pursuant to FPA section 215.

Question 6. In your view is the authority granted in the bill broad enough to protect against all cyber security threats and vulnerabilities, including those originating on distribution systems and in Alaska and Hawaii?

Answer. Yes, for the reasons explained in response to Question No. 1, above.

RESPONSES TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. The industry witnesses before us today urge Congress not to broaden federal jurisdiction in the cyber arena to extend to the local distribution system.

But, if Congress limits any new federal authority to the Bulk Power System, aren't we leaving cities like New York and Washington vulnerable to a cyber attack?

Answer. Yes, the current definition of Bulk Power System leaves certain cities, such as New York, vulnerable to a cyber attack. When. NERC proposed its first set of reliability standards, it asked that the applicability of the reliability standards be limited to facilities generally rated at 100 kV and above subject to the individual determinations of the regions. In Order No. 693, the Commission accepted this proposal but expressed concern about potential gaps in coverage. Since then, the regional definition applicable to Washington, D.C., has been strengthened adequately to include the transmission systems serving the city, but a different regional definition excludes most of the network facilities in the New York City area. Moreover, the Bulk Power System is statutorily defined as excluding facilities used in local distribution. The draft bill's language is broader than the Bulk Power System and would allow the Federal government to protect against such a gap.

Question 2. In the 2005 Energy Policy Act, Congress created an Electric Reliability Organization—which is now NERC—to develop mandatory and enforceable reliability standards, including cyber security standards, for the electrical grid. While this "Section 215 Process" provides for extensive stakeholder involvement, FERC has complained that the process is too time-consuming, does not allow timely changes, and does not protect security-sensitive information. I am concerned that even though we learned about Aurora in 2007, the NERC standards will still not be in place until 2010. Do the witnesses agree that the additional federal authority, beyond the Section 215 process, is needed for cyber security protection?

Answer. Yes.

Question 3. Section 215 of the Federal Power Act gives FERC the authority to oversee mandatory, enforceable reliability standards for the Nation's bulk power system, but excludes Alaska and Hawaii. What are the challenges in including Alaska, Hawaii, and the territories in cyber security action?

Answer. The Commission would need to learn about the facilities that provide electric service in these States and territories, and establish a communication protocol to convey information and directives.

Question 4. We can have the most secure systems here in the U.S., but we are interconnected with our northern and southern neighbors. What kind of coordination do we have with Canada and Mexico today? How much of an impact on the U.S. would there he from a cyber-intrusion into the Canadian or Mexican systems?

Answer. The Commission and DOE maintain close coordination with Canadian and Mexican governmental officials and regulators; representatives from the three countries communicate by telephone or meet frequently. Officials in Canada and Mexico are well aware of the risks of cyber-intrusion, and the need to protect against such vulnerabilities and threats. The impact on the United States from a cyber-intrusion in Canada or Mexico is difficult to predict, and could vary widely based on the nature and location of the intrusion, as well as the system conditions at the time an intrusion occurs or is activated.

Question 5. Some of the industry witnesses have argued that Congress should provide emergency/expedited authority to either DOE or FERC—but not both. How do you respond?

Answer. The comments that supported giving the authority to either FERC or DOE but not both seemed to flow from a concern that there would be an overlap. However, the draft bill authorizes FERC to address vulnerabilities while authorizing DOE to address threats, so it is not clear that there will be an overlap. If circumstances arose in which the statute allowed both agencies to act, the agencies would need to coordinate their efforts appropriately, and I believe the agencies would act timely and responsibly in doing so. The FERC, which currently is the Federal agency statutorily responsible for overseeing reliability, has the expertise and processes in place to timely and effectively issue orders directing necessary actions to address reliability vulnerabilities or to address threats in emergency situations, to ensure that the actions ordered do not conflict with other reliability requirements, and to enforce its orders. The FERC also has many years of experience in reacting promptly to industry urgent action needs.

Question 6. You testified that the legislation should address not only cyber security threats but also extend to other national security threats to reliability. What additional authority does FERC require?

Answer. Physical or non-cyber events or attacks can damage the grid as much as, or more than, cyber attacks. While law enforcement agencies may be able to inform utilities about known or suspected threats, and provide or enhance protection against certain threats, I am unaware of any federal agency or law enforcement agency with authority to require utilities to take preventative actions to mitigate non-cyber vulnerabilities or threats to the power grid even if they endanger national

security. It is impossible to speculate as to what specific non-cyber vulnerabilities and/or threats might materialize in future years, although it is certain that when such issues arise, it cannot be assured that they will be dealt with in a timely and effective manner unless a Federal agency is already authorized to require appropriate action. These non-cyber 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. Broadening the draft bill to include 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. If the Congress does not enact a provision to enable the Commission to act to protect the power grid from such threats, there will be a gap in protection of the grid.

Question 7. When FERC issues an alert or advisory for industry to take a voluntary action, such as in response to the Aurora vulnerability, what is the compliance rate?

Answer. I am not aware of calculations of compliance rates, since some NERC issuances do not recommend specific actions and all are merely voluntary. NERC, and not FERC, issues alerts to address vulnerabilities or threats that are not covered by the reliability standards. Since the Aurora advisory, NERC has restructured its alert process, with Commission oversight. NERC now has three levels of alerts, and also issues awareness bulletins. Not all alerts require any feedback from industry. The three alert levels are: Industry Advisories, Recommendations to Industry and Essential Action Alerts. The Essential Action Alerts are the highest urgency alerts, and are most like the Aurora alert. Since putting this mechanism in place, no Essential Action Alerts have been issued. Voluntary compliance with these advisories has not been the subject of any audit—by NERC or the Commission. Thus, the effectiveness of these alert efforts is uncertain.

ATTACHMENT

I. Changes to Address Non-Cvber Vulnerabilities or Threats

A. In section (b)(1), after "cyber security vulnerabilities" insert "or other national security vulnerabilities".

B. In section (h)(2), after "a cyber security vulnerability" insert "or national security vulnerability".

C. In section (c)(1), after both references to "cyber security threat" insert "or national security threat".

II. Changes to Broaden Protection of CEII

Revise section (f) by adding the text underlined below:

> Section 214 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 133) shall apply to critical electric infrastructure information submitted to, or developed by, the Commission or the Secretary under this section to the same extent as that section applies to critical infrastructure information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 131 et seq.) If a rule or order issued pursuant to this section contains critical electric infrastructure information or if information in the record associated with such rule or order constitutes critical electric infrastructure information, the Commission or the Secretary may make the rule, order or information non-public in whole or in part.

RESPONSES TO QUESTIONS FROM SENATOR BAYH

Question 1. In your agency's view, would the proposed legislation drafted by the Committee on Energy and Natural Resources be complementary of various other legislative efforts to address the issue of cyber security in other sectors (banking, commerce, military, and intelligence)?

Answer. Yes, the proposed legislation would be complementary to other legislative efforts addressing cyber security in other sectors such as banking, commerce, military, and intelligence. The legislation directs 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 these matters. It 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. I believe

that in order to be 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, NRC, CIA and others 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.

Question 2. If this legislation is enacted, how would new DOE and FERC authorities be complementary of the other efforts to ensure cybersecurity undertaken by the Executive Branch and of each other?

Answer. As I mentioned previously, even if Congress or the President were to create a central authority, FERC expects to coordinate as appropriate with that authority to effectively establish and implement cyber security measures necessary to address vulnerabilities. Should the proposed draft retain the separation of FERC and DOE responsibilities, FERC expects to coordinate with DOE in order to prevent overlap of our orders and enforcement actions regarding FERC's responsibility to address "vulnerabilities" and DOE's responsibility to address "threats". Again, FERC already coordinates with many other agencies such as DOE, DoD, DHS, NRC and CIA to avoid duplicative or conflicting actions. At times, as during Aurora, FERC worked closely with the Executive Branch which convened interagency meetings to coordinate the actions of all federal agencies in order to assure an effective and comprehensive plan. Therefore, action to formalize an Executive Branch role is not expected to cause a conflict, overlap or other adverse effect on FERC's role.

Question 3. Currently, how are DOE and FERC coordinating with all of the other agencies and departments involved in cyber security (for example, DHS, DoD, and the Intelligence Community)?

Answer. In addition to excellent working relationships and issue-based contacts between staff members of FERC, DOE, DoD, DI IS, CIA, and NSA, there are several formal processes that engage our agencies.

a. FERC participates as a member of the Energy Sector Government Coordinating Council co-chaired by DOE and DHS. The Council is organized to coordinate security activities of federal agencies in the Energy Sector. The Council also facilitates interaction with the energy industry's members through their sector coordinating councils.

b. Defense Science Board—I have served as a resource to the energy task force evaluating specific physical and cyber vulnerabilities and their impact to the mission-critical functions of the armed services. As part of this assignment, I have helped to conduct briefings of the Senate's Armed Services staff members as well as briefings of senior DoD officials at the Pentagon.

c. Joint Projects and Studies—FERC has conducted independent studies and has initiated joint studies with other agencies such as DOE, DoD, and others to evaluate physical and cyber security vulnerabilities and to identify effective mitigation techniques.

d. Memorandums of Understanding—FERC has executed an MOU with the NRC and meets with staff to discuss cyber security issues of the power grid and how they could affect the operation and security of the nuclear power plants. In fact, FERC just recently issued an order after considering comments, including from the NRC staff, to eliminate a gap in regulatory coverage of cyber security standards in the "balance of plant" portion of nuclear generating plants not directly related to the nuclear safety, security or emergency preparedness.

e. Industrial Control Systems Joint Working Group (the WG)—FERC participates in the WG that is organized and run by DHS. The WG encompasses cyber security issues for all sectors, and involves governmental and industry organizations.

Question 4. How will these efforts be affected by the President's cybersecurity review?

Answer. We have not yet seen the President's cybersecurity review and therefore cannot comment on its effect on our responsibility regarding the Bulk Power System or its interaction with the proposed legislation. However, I can reiterate that FERC is a regulatory agency and is expert at crafting orders, issuing them quickly when necessary, conducting fair proceedings for the regulated community, and enforcing its orders and directives. FERC has the statutory responsibility to oversee the reliability and cyber security of the nation's power grid. I believe that any new cyber security initiative or review should consider FERC's statutory responsibility and expertise to protect the electric infrastructure that our country depends upon for its safety, economy, and military preparedness. Should the proposed legislation pass, I expect that this will complement FERC's existing authorities to protect reliability of the transmission grid by allowing FERC to immediately address vulnerabilities

to the Nation's critical electric infrastructure. In the event that the President's cybersecurity review leads to the creation of a new Executive Branch role, as in the past FERC would coordinate with this function to assure that its actions are effective and comprehensive in the context of the actions of the other agencies.

RESPONSES OF ALLEN MOSHER TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. In your view is the authority granted in the proposal sufficiently broad to allow protection against all cyber security threats and vulnerabilities? Does the provision cover Alaska, Hawaii, and distribution systems?

Answer. APPA has assumed that the question is directed to cyber security threats to and vulnerabilities on the electric system. Based on that premise, the proposal, through the Section 224(a)(1) definition of "Critical Electric Infrastructure," is sufficiently broad to allow protection against cyber security threats and vulnerabilities to electric system assets, including generation, transmission and distribution. In fact, APPA is concerned that the scope of the proposed authority is overly broad, in that the inclusion of distribution facilities may tax the scarce resources needed to mitigate risks associated with attacks on the bulk power system.

APPA is also concerned that the scope of this authority may not be clearly delineated and may overlap with authorities reserved to state and local regulatory bodies. APPA continues to oppose granting emergency authorities to FERC over distribution facilities.

The phrase at page 1, line 10, "affecting interstate commerce" could be interpreted to imply that the covered distribution facilities may be used to provide electric service in interstate commerce. Under that interpretation, Hawaii and Alaska would not be covered by the proposal.

But the text "affecting interstate commerce" could also be interpreted to imply that interruption of service through attacks on critical electric infrastructure would have a debilitating impact on the operations of electric customers. In that event, Alaska, Hawaii and all distribution electric assets, including private networks owned by non-utilities, might be covered.

Question 2. You agree that it would be appropriate for FERC to issue "interim measures" to protect against the Aurora vulnerability. Do you not believe that there are other vulnerabilities that deserve this same treatment? What if, next week, we discovered eight others? Should we not allow FERC to issue interim measures for all vulnerabilities?

Answer. APPA's support for FERC authority to address the Aurora cyber-security vulnerability is based on the recognition that current NERC Critical Infrastructure Protection reliability standards do not encompass all bulk-power system facilities and that the Aurora Advisory identified certain vulnerabilities that can and should be addressed now. The primary message of the Aurora advisory—that utilities should secure utility operating data and control systems from unauthorized remote access—is fundamental. One important set of lessons to be learned from Aurora is that advisories need to be clearly describe the nature of the vulnerability and that not all recommended mitigation measures work in all situations. The Aurora advisory process then in existence lacked the needed processes to clarify or refine the actual advisory and receive feedback from industry experts before it was issued to the industry as a whole.

A comprehensive set of mandatory reliability standards will provide a framework for systematic analysis and response by bulk power system asset owners to new vulnerabilities. Thus, as specific new vulnerabilities emerge in the future, they can and will be addressed, either through new NERC standards for the bulk power system or through the development of interpretations of then-existing CIP standards. FERC's existing authority under FPA Section 215 to direct NERC to submit a new or revised reliability standard addressing a specific matter, in conjunction with improved government-industry communication processes should obviate the need for FERC authority to direct interim measures.

Question 3. We have included the sensitive information protections from the Critical Infrastructure Information Act. Are these protections not sufficient? If not, what would be?

Answer. No. Unfortunately, the Critical Infrastructure Information Act appears to protect only voluntary data submittals by private sector entities to the Department of Homeland Security and possibly other federal agencies. Submittals required by regulatory orders, data exchanged by private sector entities, information exchanged among entities during NERC standards development processes, and communications by federal, state, municipal and other locally owned utilities with third parties do not appear to be covered by the referenced act.

APPA recommends that the Committee examine closely the language of Section (f) of H.R. 2165, introduced into the House of Representatives by Rep. Barrow on April 29, 2009.

APPA will also provide additional draft statutory language to address the particular concerns of state and locally-owned utilities as soon as possible.

RESPONSES OF ALLEN MOSHER TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. The industry witnesses before us today urge Congress not to broaden federal jurisdiction in the cyber arena to extend to the local distribution system. But, if Congress limits any new federal authority to the Bulk Power System, aren't we leaving cities like New York and Washington vulnerable to a cyber attack?

Answer. On balance, no. Protecting the bulk power system from cyber attack necessarily entails taking measures to ensure that the bulk power system is not vulnerable to attacks originating on the interconnected distribution system. Such attacks could be propagated either through utility system data and control systems used perform both transmission and distribution functions, or through attacks on customer devices that might be propagated upward and adversely affect power characteristics on the bulk power system (e.g., real and reactive power demands, frequency, voltage, etc.). In the former case, integrated utilities have an interest in protecting both their transmission and distribution systems from attack and will apply cyber security measures throughout their systems. In the latter case, proper design and certification of Smart Grid devices will ensure that cyber-security capability is built in rather than added in a patchwork process after the fact. Finally, distributions utilities in major cities and their retail regulators will respond to threat and vulnerability information made available through NERC ES-ISAC and DOE information sharing and analysis programs.

Question 2. In the 2005 Energy Policy Act, Congress created an Electric Reliability Organization—which is now NERC—to develop mandatory and enforceable reliability standards, including cyber security standards, for the electrical grid. While this "Section 215 Process" provides for extensive stakeholder involvement, FERC has complained that the process is too time-consuming, does not allow timely changes, and does not protect security-sensitive information. I am concerned that even though we learned about Aurora in 2007, the NERC standards will still not be in place until 2010. Do the witnesses agree that the additional federal authority, beyond the Section 215 process, is needed for cyber security protection?

Answer. As I noted in my testimony, APPA supports authority for FERC to issue emergency orders in response to an imminent threat. APPA also supports authority for FERC to direct entities subject to Section 215 to take interim measures to secure their bulk power system assets from the vulnerabilities described in the Aurora advisory.

APPA also agrees that the NERC standards development process can be complex and time consuming. Nonetheless, APPA fully supports Congress' decision in the Energy Policy Act of 2005 to rely upon the Section 215 model of an industry-based Electric Reliability Organization—NERC—to develop reliability standards that are technically sound, well understood and broadly supported by the 1800 entities within the electric power industry that have to live with these standards on a day-to-day basis. The additional time required to develop standards through this process helps ensure that technical issues are resolved up front by industry experts and that potential unintended consequences (such as a cyber-security rule that might impair real time operating procedures) are addressed early on.

NERC has adopted procedures that provide for emergency standard development to quickly fill gaps that may be identified in existing reliability standards. NERC's rules of procedure and reliability standards development process provide for a two-step response. Where the nature of the underlying threat or vulnerability and the associated mitigation measures are well-defined, cyber-security experts from NERC and the electric industry collaborate with federal government agencies and other sources (e.g., US-CERT) to craft an advisory with recommended or essential actions to be taken by the applicable entities (generally owners and operators of the potentially affected bulk power system assets). Essential action advisories must be approved by the NERC Board of Trustees. Each entity that receives an essential action or recommended action advisory must respond to NERC that it has received the advisory and must describe the actions it has taken. If the underlying threat or vulnerability is sustained in nature and is not addressed by an existing reliability standard, an emergency standards development process can be initiated resulting in the development and approval of a new or revised reliability standard within days.

APPA does believe that existing law makes it difficult to protect security-sensitive information during the standards-development process. This would appear to be

true regardless of whether such standards were developed by stakeholders through NERC's standards development procedure or by and FERC through some form of public notice and comment. FERC witness Joseph McClelland raised similar concerns.

Question 3. You mentioned the need for a greater flow of information from the government to industry on cyber security threats. What is the current process/course of action for cyber security threats for the private sector? Why do you want DOE as the lead and how would having a Cyber Security Czar in the White House impact that flow of information?

Answer. APPA suggests that NERC is better equipped than APPA to provide a full description of its processes and responsibilities as the ES-ISAC. See the response to Question 2 for a brief overview.

APPA sees several advantages to placing DOE in the lead role with respect to communications with the electricity sector. First, DOE has that role as the Government Coordinating Council for the energy sector today. DOE both understands the energy sector and has access to high-level intelligence information from other cabinet-departments and intelligence agencies, allowing it to act as a conduit, filter and translator of intelligence threat and vulnerability information into actionable forms that may be used by the electric utility industry. Finally, as described by DOE witness Patricia Hoffman, the Department is the federal agency that is best situated to help improve the technological state of the art in cyber-security, while advancing other important energy policy goals such as the deployment of Smart Grid technologies.

APPA does not have a position on whether a Cyber Security Czar should be established in the White House or whether the flow of threat and vulnerability information from government to industry might be improved by such an action. APPA merely observes that a narrow, surgical approach to addressing cyber security issues based on existing FERC and DOE authorities would be less likely to come into conflict with Congressional and Executive Branch decisions on how to better align the federal government's cyber-security strategy as a whole.

Question 4. It has been suggested that the draft legislation we are considering could be duplicative and cause confusion by giving parallel powers to DOE and FERC for cyber security threats and vulnerabilities. How does the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) fit into the picture in disseminating these potential new rules and orders to the electricity industry? Does information flowing through this Center help reduce any confusion or is it more about which agency has the lead?

Answer. APPA suggests that NERC is better equipped than APPA to provide a full description of its processes and responsibilities as the ES-ISAC. See the response to Question 2 for a brief overview.

APPA believes information should continue to flow through the ES-ISAC regardless whether such information originates within the federal government or from public-private partnership arrangements, universities or equipment vendors and manufacturers. Under the current legal framework, the ES-ISAC is responsible for issuing alerts to the entire electric sector. These alerts are described as advisories, recommendations or essential actions. Recommendations and essential action alerts are accompanied by suggested mitigation measures. ES-ISAC alerts are separate and distinct from NERC's responsibility as the ERO to develop and enforce mandatory reliability standards. The ES-ISAC is not structured as a body with appropriate governance, due process and compliance procedures to act as a vehicle to disseminate and ensure compliance with rules and orders.

Responses of David K. Owens to Questions From Senator Bingaman

Question 1. In your view is the authority granted in the proposal sufficiently broad to allow protection against all cyber security threats and vulnerabilities? Does the provision cover Alaska, Hawaii, and distribution systems?

Answer. The language in the joint staff draft appears intended to protect against all cyber security threats and vulnerabilities, including those affecting distribution systems and Alaska and Hawaii. However, just as it is impossible as a practical matter to absolutely guarantee 100% electric system reliability all of the time, a 100% threshold for cyber security is virtually unattainable. Perfect security is not a static, or even realistic, goal for security professionals, including those in the electric utility industry, because the technologies utilized by the industry, as well as the techniques pursued by cyber adversaries, are continuously evolving.

EEI and its member companies believe there is considerable strategic value in demonstrating to our cyber adversaries the ability to respond to a threat with swift,

unambiguous action. That is why we support designating a single federal regulatory authority that, in case of an imminent emergency threat, could issue clear actionable orders and, where necessary, enforce those orders.

In crafting legislation, Congress should try to avoid inadvertently creating a framework that could weaken grid security rather than strengthening it. For example, the inclusion of an overly broad diversity of assets and systems, as proposed in the joint staff draft, could significantly complicate the task of quickly writing unambiguous orders for actions to be taken to mitigate the threat, with significant risk that such orders would be ineffective or could cause other unintended adverse consequences. Also, attempting to address every single cyber security threat or vulnerability is inconsistent with a fundamental tenet of security, i.e., the use of risk analysis to prioritize resources. The technical comment at the end of the Department of Energy's prepared testimony submitted for the May 7 hearing is a good description of such an approach. Using a risk-based approach means protecting against threats or vulnerabilities with the highest consequences to reliability or public welfare and safety. This is why Federal Power Act (FPA) section 215 focuses on protecting the reliability of the North American bulk power system.

Question 2. Is it not true that threats to the bulk power system can come from attacks through distribution system control systems? If so, should we not protect against those possible attacks as well as those that come from transmission system control systems?

Answer. Under current North American Electric Reliability Corporation (NERC) standards, if an attack on a distribution control system could impact the bulk power system, that piece of distribution equipment would be covered by NERC standards and authority under FPA section 215. Thus, EEI would argue that protection already exists against possible attacks on the bulk power system through distribution control systems.

Responses of David K. Owens to Questions From Senator Murkowski

Question 1. The industry witnesses before us today urge Congress not to broaden federal jurisdiction in the cyber arena to extend to the local distribution system. But, if Congress limits any new federal authority to the Bulk Power System, aren't we leaving cities like New York and Washington vulnerable to a cyber attack?

Answer. No. In the Energy Policy Act of 2005, Congress wisely left the definition of the "bulk power system" flexible to allow the inclusion of assets to address special circumstances such as those posed by major cities like New York City and Washington, DC. In effect, there is not a single definition of "bulk power system" for the entire country, but instead each region has its own definition crafted to reflect the unique system design, operating and engineering characteristics, and asset makeup in that region. This flexibility provides FERC the ability to exercise discretion to include specific areas or assets, including some distribution assets where necessary for reliability purposes. In fact, FERC has pending in docket RC09-3 a filing by NERC to include additional assets in New York City, and has already acted in an earlier docket to include additional assets in Washington, DC.

Question 2. In the 2005 Energy Policy Act, Congress created an Electric Reliability Organization—which is now NERC—to develop mandatory and enforceable reliability standards, including cyber security standards, for the electrical grid. While this "Section 215 Process" provides for extensive stakeholder involvement, FERC has complained that the process is too time-consuming, does not allow timely changes, and does not protect security-sensitive information. I am concerned that even though we learned about Aurora in 2007, the NERC standards will still not be in place until 2010. Do the witnesses agree that the additional federal authority, beyond the Section 215 process, is needed for cyber security protection?

Answer. As stated in our testimony, EEI agrees that it is appropriate for Congress to provide federal energy regulators with explicit new statutory authority to address imminent and serious emergency cyber security threats. Any new authority should be narrowly tailored to deal with real emergencies; overly broad authority could undermine the collaborative framework that is needed to further enhance security.

It is important to note that current law already provides the means to address the many non-emergency cyber security issues in the electric industry. Any new emergency authority should be complementary to existing authorities under FPA section 215, a proven approach that relies on industry expertise as the foundation for developing reliability standards.

Question 3. You mention the need for manufacturers of grid equipment and systems to build security into their products. Is the electric industry able to use procurement power to persuade vendors to deliver these safe systems, or is the industry too diverse in the systems and technologies they use to have the ability to influence

product design? Isn't part of the problem that many of these systems are manufactured overseas?

Answer. Procurement contracting is one way the industry can attempt to get vendors to build additional security into their products. However, EEI believes that building security into electric utility systems is too important to deal with solely on a contract-by-contract basis. Relying on this approach assumes that every utility has adequate expertise to negotiate in the procurement process for appropriate security protections, and that every vendor has adequate expertise to fulfill requirements made by the customer. The experience of EEI members has not shown these assumptions to be true. EEI believes that a uniform set of appropriately rigorous testing criteria, administered by a third party expert who would certify that the criteria had been applied and passed, would mitigate these issues.

The National Institute of Standards and Technology (NIST) effort to develop a smart grid interoperability framework offers opportunities in this area. NIST plans to develop vendor and manufacturer certification guidelines as part of the third phase of this effort. Overseas manufacturers could be subject to the same certification processes.

Another advantage of smart grid vendor and manufacturer security verification is that it could help state utility regulators objectively evaluate utilities' capital expenditures for inclusion of reasonable cyber security as a criterion for cost recovery purposes. This also could help indirectly encourage manufacturers of grid equipment and systems to build security into their products.

Question 4. You have stressed that information sharing on the government's part is a vital component in cyber security. Which federal and state agencies/departments do you coordinate with on cyber security threats and vulnerabilities? Are there instances when intelligence and law enforcement officials have not shared actionable information in a timely manner?

Answer. The electricity industry coordinates with and has received classified briefings from many federal agencies on cyber security issues, including the FBI, DHS, DOE, FERC, the NRC, CIA, Department of Commerce, DoD, and ODNI. Many agencies, in particular DOE, also work closely with industry personnel to educate and assist them in developing strong cyber security strategies. Electric utilities are eager to learn any information that helps them more effectively and efficiently secure their systems, and EEI very much appreciates the efforts of these agencies in helping utilities improve their cyber security.

EEI believes that Congress should encourage a consultative relationship between utilities and government agencies as a necessary component of securing systems, and should not rely solely on a broad regulatory approach to achieve effective security. It is inevitable that the most sophisticated expertise on addressing the latest cybersecurity threats will rest in federal agencies with national security responsibilities. This information cannot be made available to electric utility personnel, who nevertheless under the proposed legislation could be expected to share responsibility for national security. Expertise in reliably and safely operating electricity assets in a large integrated system rests within the electric utility industry. EEI believes that security is enhanced by leveraging both types of expertise to identify efficient and effective techniques for securing electric industry systems.

Question 5. A company in Alaska tells me that it is possible to put a one-way regulator on cyber networks so information can flow out from the network to managers that need access to the data, but data cannot be sent back into the network from a remote source—ie: an outside attack. Do you view a one-way flow regulator as a feasible solution?

Answer. There are solutions that can be placed on networks which allow a secure one-way communication of data between networks of different security levels. This is a feasible option, which is already being used by some utilities, but only as part of an overall defense-in-depth cyber security program.

RESPONSES OF RICHARD P. SERGEL TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. In your view is the authority granted in the proposal sufficiently broad to allow protection against all cyber security threats and vulnerabilities? Does the provision cover Alaska, Hawaii, and distribution systems?

Answer. The jurisdictional scope described in the Joint Staff Draft is the broadest that I can conceive. It covers generation, transmission, and local distribution. It covers Alaska and Hawaii. The use of the phrase "affecting interstate commerce" has been construed by the U.S. Supreme Court to be coterminous with the full extent of the Congress's authority under the Commerce Clause of the U.S. Constitution. Thus, I don't see that anything is left out. If Smart Grid devices were implicated

in a cyber threat or vulnerability, they would be covered. As well, the language appears broad enough to reach third-party communications providers if they were implicated in any threat or vulnerability. Because I do not have access to information regarding the full range of cyber security threats and vulnerabilities facing the United States, I cannot say whether the proposed Joint Staff Draft grants sufficient authority to allow protection against "all cyber threats and vulnerabilities."

Question 2. You suggest that we should not give FERC authority to establish standards pending the outcome of your deliberations. Do you not think that it is important to protect these critical assets during the years that it takes to get a standard through your organization?

Answer. NERC believes the Congress should adopt legislation granting an agency of the Federal government emergency authority to address an imminent cyber security threat. Each of the examples given in testimony by the witness for the Federal Energy Regulatory Commission involved situations where the action needed to occur to address "threats to national security quickly" and "require immediate action" (Prepared Testimony of Mr. McClelland, page 8), as well as when "there may be a need to act decisively in hours or days" (Prepared Testimony of Mr. McClelland, page 9). That is what emergency authority is all about. A grant of emergency authority, such as that granted to the Department of Energy under the draft legislation, will provide the Federal government the authority it needs to address any specific situation that must be addressed in "hours or days."

NERC now has in place a baseline set of standards designed to protect the security of the bulk power system. NERC's Critical Infrastructure Protection standards cover these broad categories:

- Sabotage Reporting
- Critical Cyber Asset Identification
- Security Management Controls
- Personnel & Training
- Electronic Security Perimeter(s)
- Physical Security of Critical Cyber Assets
- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plans for Critical Cyber Assets

These nine standards, encompassing roughly 45 individual requirements, are already in effect. Audits for compliance with 13 requirements in these standards will begin for a certain set of entities on July 1, 2009, with audits beginning for the remaining requirements and remaining entities in 2010.

NERC and the industry are working to improve and strengthen those standards, including addressing the modifications directed by FERC in Order No. 706. NERC, working with industry security and operations experts and FERC staff, has divided that work into two concurrent phases. Last week, industry stakeholders approved phase one of the improvements by an 88% affirmative vote. On May 6, 2009, the NERC Board of Trustees approved those phase one revisions to the Critical Infrastructure Protection standards. These revisions will be filed shortly with FERC for approval and, if approved, they will become binding and enforceable. Phase two revisions are already underway and are expected to be complete in 2010. NERC and industry experts will continue their work to improve those standards further in the months ahead.

Please note that NERC has procedures that enable it to adopt standards in substantially less time than "years." To respond to the need for standards to address pressing reliability or security concerns, NERC can employ its urgent action standards development process. Under its current construct, a proposed standard can be processed through approval in approximately two months. Modifications to this timeline are under review and are to be presented for NERC Board approval in early August. These changes would dramatically reduce this approval timeframe to as few as 10 days once a team drafts the proposed standard. These timelines are impacted by the time needed to craft the standard in response to the identified threat or vulnerability.

If NERC needs to develop a reliability standard in response to a critical issue that is so confidential that information can only be shared on a "need to know" basis, NERC will use all the steps in the standards development procedure, but will limit the participation and the amount of information released within some of the steps of the procedure. This balances the need to preserve the integrity of the reliability standards development procedure with the need to preserve the confidentiality of information that, if exposed, could put the reliability of the bulk power system at risk.

Question 3. Do you know how long it will be before NERC is able to address the weaknesses in the standards remanded by the Commission?

Answer. The Commission did not remand NERC's Critical Infrastructure Protection standards. Instead, the Commission approved those standards, stating:

> In approving the CIP Reliability Standards, the Commission concludes that they are just, reasonable, not unduly discriminatory or preferential, and in the public interest. These CIP Reliability Standards, together, provide baseline requirements for the protection of critical cyber assets that support the nation's Bulk-Power System. Thus, the CIP Reliability Standards serve an important reliability goal. Further, as discussed below, the CIP Reliability Standards clearly identify the entities to which they apply, apply throughout the interconnected Bulk-Power System, and provide a reasonable timetable for implementation. (Order No. 706, para. 24.)

Those standards are now in effect. Users, owners, and operators of the bulk power system are in the process of coming into compliance with those standards, in accordance with the implementation timetable approved by the Commission. In Order No. 706, the Commission also directed NERC to make a number of improvements in the Critical Infrastructure Protection standards, and NERC is in the process of doing that now.

As described in my response to the prior question, this week NERC's Board of Trustees approved the first phase of the improvements to the standards directed by the Commission. The phase one improvements include removal of the "reasonable business judgment" test and the "assumption of risk" criterion. The improvements also strengthen senior management's accountability for implementation of critical infrastructure protection programs within each company. Related procedural rules will provide for audits of technical feasibility exceptions claimed by users, owners, and operators of the bulk power system. NERC and industry security and operations experts are now working on the second phase of the improvements directed by the Commission. NERC expects to complete phase two during 2010.

Responses of Richard P. Sergel to Questions From Senator Murkowski

Question 1. The industry witnesses before us today urge Congress not to broaden federal jurisdiction in the cyber arena to extend to the local distribution system. But, if Congress limits any new federal authority to the Bulk Power System, aren't we leaving cities like New York and Washington vulnerable to a cyber attack?

Answer. The greatest risk to the Nation is threats to the bulk power system, and Congress should make sure that risk is addressed. State commissions and local authorities can act to protect local distribution facilities if they have access to prompt actionable information on which to base any requirements they might impose. However, the vast majority of the information about the risks and threats to the electric system is in the hands of Federal authorities, and much of that information is classified. Getting actionable intelligence and mitigation measures in the hands of state and local officials who already have authority to act to protect the cyber security of their cities is the best way to protect those localities.

Question 2. In the 2005 Energy Policy Act, Congress created an Electric Reliability Organization—which is now NERC—to develop mandatory and enforceable reliability standards, including cyber security standards, for the electrical grid. While this "Section 215 Process" provides for extensive stakeholder involvement, FERC has complained that the process is too time-consuming, does not allow timely changes, and does not protect security-sensitive information. I am concerned that even though we learned about Aurora in 2007, the NERC standards will still not be in place until 2010. Do the witnesses agree that the additional federal authority, beyond the Section 215 process, is needed for cyber security protection?

Answer. NERC believes the Congress should adopt legislation granting an agency of the Federal government emergency authority to address an imminent cyber security threat. Each of the examples given in testimony by the witness for the Federal Energy Regulatory Commission involved situations where the action needed to occur to address "threats to national security quickly" and "require immediate action" (Prepared Testimony of Mr. McClelland, page 8), as well as when "there may be a need to act decisively in hours or days" (Prepared Testimony of Mr. McClelland, page 9). That is what emergency authority is all about. A grant of emergency authority, such as that granted to the Department of Energy under the draft legislation, will provide the Federal government the authority it needs to address any specific situation that must be addressed in "hours or days."

Standards are different, because they prescribe the actions and practices that all entities, large and small, must follow day in and day out. Standards-setting is intentionally a deliberative process that involves the application of expertise in many disciplines. Entities may be subject to fines of up to $1,000,000 per day per violation

for failure to comply with standards. The electricity production and delivery system is technically very complex, so it is important in establishing standards that there be no unintended consequences that may actually reduce the reliability or security of the system. NERC now has in place a baseline set of standards designed to protect the security of the bulk power system. NERC's Critical Infrastructure Protection standards cover these broad categories:

- Sabotage Reporting
- Critical Cyber Asset Identification
- Security Management Controls
- Personnel & Training
- Electronic Security Perimeter(s)
- Physical Security of Critical Cyber Assets
- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plans for Critical Cyber Assets

NERC and the industry are working to improve and strengthen those standards, including addressing the modifications directed by FERC in Order No. 706. NERC, working with industry security and utility experts and FERC staff, has divided that work into two concurrent phases. Last week, industry stakeholders approved phase one of the improvements by an 88% affirmative vote. On May 6, 2009, the NERC Board of Trustees approved those phase one revisions to the Critical Infrastructure Protection standards. NERC and industry experts will continue their work to improve those standards further in the months ahead.

To respond to the need for standards to address pressing reliability or security concerns, NERC can employ its urgent action standards development process. Under its current construct, a proposed standard can be processed through approval in approximately two months. Modifications to this timeline are under review and are to be presented for NERC Board approval in early August. These changes would dramatically reduce this approval timeframe to as few as 10 days once a team drafts the proposed standard. These timelines are impacted by the time needed to craft the standard in response to the identified threat or vulnerability.

If NERC needs to develop a reliability standard in response to a critical issue that is so confidential that information can only be shared on a "need to know" basis, NERC will use all the steps in the standards development procedure, but will limit the participation and the amount of information released within some of the steps of the procedure. This balances the need to preserve the integrity of the reliability standards development procedure with the need to preserve the confidentiality of information that, if exposed, could put the reliability of the bulk power system at risk.

Question 3. Why isn't the existing Section 215 process sufficient to address cyber security threats and vulnerabilities? Should we extend any new authority to physical assets?

Answer. As indicated in my response to earlier questions, the Section 215 standards-setting process cannot adequately deal with imminent cyber security threats. Standards prescribe the actions and practices that all entities, large and small, must follow, day in and day out. They are not capable of dealing with specific, targeted imminent threats that must be addressed "in hours or days." Granting an agency of the Federal government authority to deal with emergency threats will address the gap that currently exists. With authority to deal with emergency situations in place, NERC can continue to work through its more deliberative standards development process, using security and operations experts, to make continuous improvements in the underlying standards. NERC does not believe it is necessary for Congress to extend new authority for the protection of physical assets. Sufficient authorities and agencies already exist to deal with risks to physical assets, including local and state police, the Federal Bureau of Investigation, and the Departments of Defense and Homeland Security.

Question 4. In your written testimony, you say that in the case of an imminent cyber security threat, authority to direct action should be vested, as appropriate, in the Federal government of Canada. Could you please describe a scenario where the Canadian Government should have the authority to direct action? Directed at companies operating within the United States?

Answer. I did not mean to suggest the Canadian government should have any authority to issue directives to companies operating within the United States. Rather, my testimony reflected that fact that the interconnected bulk power system is international in scope. It spans both the U.S./Canadian border and the U.S./Mexican border. Just as NERC believes it imperative that the U.S. Federal government have emergency authority to deal with imminent cyber security threats, NERC also believes that appropriate governmental authorities within Canada and Mexico should

exercise emergency authority for imminent cyber security threats within their respective jurisdictions. The international, interconnected nature of the bulk power system does mean it is critical for authorities in all jurisdictions to coordinate their actions in dealing with imminent cyber security threats, so that they do not unintentionally cause unintended consequences that occur as a result of the actions they do require.

Question 5. Could you expand on the education challenges the industry faces in ensuring that each entity understands the cyber security challenges facing them and efforts that are being made to overcome those challenges?

Answer. The electricity industry is very accustomed to dealing with risks to the bulk power system, and users, owners and operators deal with risks such as severe weather, forest fires, mechanical breakdowns, and equipment failure every day. The cyber security challenges are different in kind, because they can be intentional, targeted attacks from remote locations, perhaps by hostile nation-states. And unlike the other location-specific risks that users, owners, and operators are accustomed to dealing with, the cyber security challenges can be very broad in scope and affect multiple assets simultaneously. The implications of this difference impact traditional thinking at a very basic level: even the criteria used to define a "critical asset" in the cyber world are different than those typically applied in traditional planning and operating analysis.

Within the last year, NERC has worked extensively to help the industry better understand the potential risks associated with significant cyber vulnerabilities. These efforts have taken a number of forms, but began with NERC's formation of a Critical Infrastructure Protection program. In August of 2008, NERC hired security expert Michael Assante as Chief Security Officer ("CSO") to lead the program and has recently brought additional expertise on board to support his efforts.

NERC has also formed an Electricity Sector Steering Group comprising seven CEO-level executives from all sectors of the electric industry to provide overall policy guidance to NERC's Critical Infrastructure Protection Program and achieve greater CEO-level buy-in from industry executives. This group first met at NERC's 2008 Cyber Security Summit held in coordination with four government agencies in September 2008. The event was attended by 130 industry executives and covered various security-related topics. In addition to this initial session, NERC has subsequently arranged for special and classified briefings for industry executives in the United States and Canada with the intelligence community. NERC expects to continue this outreach, with another session currently being planned for December 2009.

Webinars and other communications materials have been another key component of NERC's educational outreach. NERC's CSO has spoken at a number of industry web-based and in-person events. NERC has also given significant support to the organization of security conferences, such as the SCADA Summit meeting held in conjunction with the annual SANS Summit in February. Additionally, NERC is currently developing a five-part webinar series designed to educate stakeholders about requirements in NERC's CIP standards.

NERC's alerts mechanism has acted as yet another educational tool. In addition to their primary role of providing actionable information to industry, regular issuance of advisories has certainly helped to sensitize the four to five thousand individual alert recipients to these issues. In addition to its alerts, NERC has also begun to issue critical infrastructure "awareness bulletins" regarding critical infrastructure concerns as they arise.

In February of 2009, NERC also launched its "Network Hydra," a network of industry security professionals who are regularly convened via conference call and e-mail to discuss emerging cyber security issues.

NERC also facilitates its Critical Infrastructure Protection Committee, a group of approximately thirty industry professionals dedicated to discussing and producing guidance related to critical infrastructure concerns to the industry. The group meets face-to-face quarterly and via conference call as necessary. NERC staff is in close coordination with the "Executive Committee" of this Committee on a weekly basis. As an example of its work, the group has recently posted a set of guidelines for critical asset identification for industry comment and plans to finalize these documents in the coming months.

NERC views the standards development process itself as a key educational tool as well, as drafting the standards drives many discussions within the industry as groups seek to provide comment and vote on the standards.

Finally, regular correspondence with the industry, via letters such as CSO Michael Assante's April 7th letter, the monthly newsletter, and through a "CSO blog" that will become available on NERC's website in the coming week, also provide an important educational mechanism for the industry.

RESPONSES OF PATRICIA HOFFMAN TO QUESTIONS FROM SENATOR BINGAMAN

Question 1. In your view is the authority granted in the proposal sufficiently broad to allow protection against all cyber security threats and vulnerabilities? Does the provision cover Alaska, Hawaii, and distribution systems?

Answer. The proposed language gives the government new authority to require entities that own and operate the electric power system to address newly discovered vulnerabilities and threats. The definition of critical infrastructure in the proposed language is sufficiently broad to encompass Alaska, Hawaii, and distribution systems.

Question 2. Are there other vulnerabilities described in the Idaho National Laboratory report besides the Aurora vulnerability?

Answer. Yes. The Idaho National Laboratory (1NL) 2008 *Common Vulnerabilities Report* summarizes vulnerability findings from 16 control system assessments performed at the Department's National SCADA Test Bed (NSTB) from 2003-2007. INL found these vulnerabilities as part of its systematic testing program, in which they assess energy control systems for potential vulnerabilities and then work closely with vendors on specific mitigations. The Department published the common vulnerabilities (those found in at least two of the control systems tested) and the appropriate mitigation strategies to help owners and operators better protect their systems from cyber attacks. Although sensitive technical details are not included in this public report, it does provide generalized analysis and steps asset owners can take to evaluate their system and implement appropriate mitigations. Understanding the types of vulnerabilities commonly found and how to mitigate them can help protect systems currently in development, as well as those already installed in critical infrastructure applications. The report does not cover the Aurora vulnerability.

Question 3. You mention a number of efforts to develop technologies and systems to prevent cyber attacks. How can you be sure that they will be implemented by utilities?

Answer. The Department recognizes that the best way to ensure that technologies address market needs and are implemented by utilities is to work in partnership with the utility owners and operators, equipment vendors, industry associations, and the research community throughout the technology development process. For national laboratory-led projects, each lab works closely with utilities to identify the end-user requirements and then develops the fundamental technology which is typically commercialized by the private sector. For example, the Pacific Northwest National Laboratory is working with several utilities (Alliant Energy, NiSource, Progress Energy, Entergy Corporation, et al) to develop a security state visualization tool of the cyber security status on a utility communications network. The tool will provide real-time situational awareness and enhanced decision-making through fusion of advanced technologies in perimeter security, network traffic analysis, and signature-based intrusion detection. The utilities are helping to develop use cases and the system requirements.

For industry-led projects, the Department selects projects on a competitive basis and requires a minimum 20%-50% cost sharing from the private-sector partners, depending on the stage of research and development. A good example of success in this area is the Bandolier project, led by Digital Bond. Digital Bond is working closely with utilities and control systems vendors to develop security software templates for control systems. The templates are used to audit the security settings against an optimal security configuration. So far, templates have been released to audit systems from seven vendors, and are available for a nominal subscriber fee on Digital Bond's website.

The Department also ensures that technology development projects leverage industry expertise and insight through the Energy Sector Control Systems Working Group, an industry-government advisory group of technical experts that was formed under the Critical Infrastructure Partnership Advisory Council. For example, the Department conducts annual peer reviews of its cyber security projects and engages the Working Group to guide the technical and commercial direction of each project.

Question 4. Is it clear that the bulk power system can be attacked through control devices and communications systems connected to distribution systems, as well as transmission systems?

Answer. Because of the interconnected nature of electric power transmission and distribution systems, we believe it is possible for attacks at the distribution system to have an impact on the transmission system. The exact nature of these consequences is dependent on the specific scenario and the impact or consequence of a specific attack must be evaluated on a case by case basis.

RESPONSES OF PATRICIA HOFFMAN TO QUESTIONS FROM SENATOR MURKOWSKI

Question 1. The industry witnesses before us today urge Congress not to broaden federal jurisdiction in the cyber arena to extend to the local distribution system. But, if Congress limits any new federal authority to the Bulk Power System, aren't we leaving cities like New York and Washington vulnerable to a cyber attack?

Answer. States and local governments generally have jurisdiction over distribution systems. If the various State regulatory authorities don't adequately address cyber security requirements, we will continue to have a regulatory gap that could expose the electric power infrastructure to unmitigated vulnerabilities.

Question 2. In the 2005 Energy Policy Act, Congress created an Electric Reliability Organization—which is now NERC—to develop mandatory and enforceable reliability standards, including cyber security standards, for the electrical grid. While this "Section 215 Process" provides for extensive stakeholder involvement, FERC has complained that the process is too time-consuming, does not allow timely changes, and does not protect security-sensitive information. I am concerned that even though we learned about Aurora in 2007, the NERC standards will still not be in place until 2010. Do the witnesses agree that the additional federal authority, beyond the Section 215 process, is needed for cyber security protection?

Answer. Federal authority will be required beyond Section 215 for cyber security protection in emergency situations when there is a need to take action as well as to address a newly discovered vulnerability that, if exploited, would have a debilitating impact on national security, economic security, and/or public health or safety (e.g. Aurora). Because cyber security vulnerabilities (which may or may not have an impact on the electric power grid) are discovered on a routine basis, the Department also believes there must be a deliberate and comprehensive process to determine if a newly discovered vulnerability warrants emergency action. All such vulnerabilities, and potential mitigation measures, must be thoroughly evaluated on a scientific basis to determine the impact and risk to the nation in the event the vulnerability was exploited. Any decision to act or issue an order must be based on sound risk management principles and judgment coupled with engineering analysis, testing, and verification considering the characteristics of the vulnerability, the capabilities of the threat, likelihood of attack, the potential consequences to the nation should the vulnerability be exploited, and the cost of mitigation. Furthermore, prior to issuing an emergency order, any proposed mitigation action must be thoroughly and comprehensively evaluated to determine its effectiveness, impact on performance of the power grid, and possible unintended consequences. Finally, the Department believes that this determination must be made through deliberation between cabinet-level agencies including the intelligence community.

Question 3. How does the Department of Energy fit into the nation's overall cyber security structure? How do you work with FERC and what other agencies do you coordinate with? Which is the lead agency?

Answer. At the Cabinet level, the Secretary of Energy is a member of the National Security Council (NSC), whose members provide top level policy advice to the President and oversight in areas that include cyber security. The Secretary is also a member of the Homeland Security Council (HSC), which also provides top level policy oversight in cyber security. The Department participates on the Deputies committee of the NSC/HSC when they meet to provide policy oversight on cyber security, and the Department also participates on the NSC/HSC Interagency Policy Committee for the global information and communications infrastructure, a policy coordination group. DOE also has representation on a lower level interagency cyber security task force that is carrying forward some of the implementation planning from the previous Administration's Comprehensive National Cyber Security Initiative. Further, the Department's Office of Intelligence and Counterintelligence is active within the intelligence community on cyber security coordination and planning.

Under Homeland Security Presidential Directive 7, the Department leads critical infrastructure protection (physical and cyber) in the energy sector—including electricity, oil, and natural gas operations—and chairs the Government Coordinating Council (GCC) for Energy, which includes the Department of Homeland Security (DHS) and FERC. In this role, the Department works closely with industry members on the Electric and Oil & Gas Sector Coordinating Councils (SCC) to develop a Sector-Specific Plan, which outlines goals for public-and private-sector security activities, including protecting critical infrastructure from cyber threats. The Department has also formed the Energy Sector Control Systems Working Group (with representatives from the DHS National Cyber Security Division, DHS Science and Technology Directorate, the Oil and Natural Gas SCC, and the Electric SCC) that serves as the primary mechanism to oversee the implementation of the *Roadmap to Secure Control Systems in the Energy Sector*. The Department also works closely

with the Department of Homeland Security on the Cross Sector Cyber Security Working Group and the Industrial Control Systems Working Group.

Question 4. We know that making our grid smarter could also increase our vulnerability to cyber attacks. I understand that NIST is addressing the issue of cyber security as it works on the Smart Grid interoperability standards. FERC has also developed a Policy Statement on this issue. Is additional federal authority needed to deal with cyber security issues in the context of Smart Grid?

Answer. The Department is working with the private sector to develop cyber security requirements for the Smart Grid to ensure that cyber security is built into the design from technology development to deployment. The National Institute of Standards and Technology (NIST) is not developing standards, per se, but is developing an interoperability framework that will identify the types of standards that will be needed and track the status of standards for the Smart Grid. NIST is also coordinating the development of cyber security standards through the appropriate standard development organizations.

At this time, we do not foresee the need for additional federal legislation to accomplish our goal through public-private partnerships. The Department will continue to work with NIST to accelerate the development of a framework for the complete suite of interoperability standards. Once a standard is completed by the applicable standards development organization, the Federal Energy Regulatory Commission will issue a rulemaking to adopt the standard as required under the Energy Independence and Security Act of 2007.

Question 5. What role did the Department of Energy play in the President's recent interagency cyber security review?

Answer. At the request of the Director of the 60-day review team, the Department temporarily assigned a senior-level representative with extensive experience in working with the energy sector on issues related to cyber security to work directly with the interagency review team. The Department provided technical assistance, background and situational analysis, and proposed options to consider for enhancing cyber security in the energy sector. The Department also provided assistance in evaluating the status of the nation's cyber security efforts in the energy sector, an understanding of agency relationships, status of ongoing projects, and strengths and weaknesses of current partnerships. In response to several data calls, the Department also submitted an inventory of departmental expertise, programs, and funding. Finally, as principal member of the Interagency Policy Committee, the Department provided comments on the draft report that is currently under review at the policy level.

Question 6. An example was given at last week's Senate Homeland Security Committee hearing where the Chief Information Officer of the Air Force, after watching an NSA test team break into the military service's system fairly quickly, asked the NSA team to help them develop a more secure system. By asking the attacking team for assistance, they put in place a more standard configuration that blocks most attacks, allows for quick security patches, and saves them money in procurement costs. Have DOE and FERC done anything similar to this?

Answer. Yes. The Department uses a systematic method for assessing the cyber security of energy control systems using its expertise in "Red Teaming", which has evolved over decades as the steward of the nation's nuclear arsenal. The Department uses the recognized capabilities of its national laboratories to test systems from an adversarial perspective, identify vulnerabilities, and work with vendors on mitigation strategies. For example, the Department uses a Red Team approach at the National SCADA Test Bed (NSTB) to conduct vulnerability assessments of control systems (this does not include active testing on "live" production systems which could cause a system failure and loss of electricity). In partnership with numerous vendors, NSTB has performed rigorous vulnerability assessments on 90% of the current market offering of SCADA and energy management systems (EMS) in the electric sector, and 80% of the current market offering in the oil and gas sector. Through 20 test bed and on-site field assessments, NSTB has delivered vulnerability information and recommendations for security improvements to vendors including ABB, Areva, GE, OSI, Siemens, Telvent, and others. Vendors have used this information to build more secure systems and both vendors and asset owners have also used it to better secure systems already in place. Vendors have developed 11 hardened control system designs following vulnerability assessments at the Test Bed, and 31 of these are now deployed in the sector. Vendors have released several software patches for use by 82 system applications in the sector. In addition, INL releases generalized findings from vulnerability assessments in its *Common Vulnerabilities Report*, which includes mitigation strategies asset owners across the sector can use to better secure their systems. Findings from NSTB vulnerability assessments have also been translated into several training courses, including the Red

Team/Blue Team Advanced Training. In this weeklong course, nearly 80 energy sector asset owners and operators have participated in a hands-on exercise either attacking or defending a control system environment, and have learned skills and techniques they can apply immediately in their own systems.

RESPONSES OF PATRICIA HOFFMAN TO QUESTIONS FROM SENATOR BAYH

Question 1. In your department's view, would the proposed legislation drafted by the Committee on Energy and Natural Resources be complementary of various other legislative efforts to address the issue of cyber security in other sectors (banking, commerce, military, and intelligence)?

Answer. The cyber security requirements for a cyber-physical system like the electric power grid are quite different than the requirements for information systems and networks used for commerce or banking. For example, the primary cyber security driver for the banking sector is to protect the confidentiality of the data. For many elements in the power grid, availability of data is the primary driver.

Question 2. If this legislation is enacted, how would new DOE and FERC authorities be complementary of the other efforts to ensure cybersecurity undertaken by the Executive Branch and of each other?

Answer. The proposed legislation provides the DOE emergency authority to address an imminent threat and provides FERC emergency authority to address vulnerabilities. The Administration is currently conducting a cyber review across the federal government and since the report has not been issued, the Department cannot comment on how the proposed efforts would be affected.

At the Cabinet level, the Secretary of Energy is a member of the National Security Council (NSC), whose members provide top level policy advice to the President and oversight in areas that include cyber security. The Secretary is also a member of the Homeland Security Council (HSC), which also provides top level policy oversight in cyber security. The Department participates on the Deputies committee of the NSC/HSC when they meet to provide policy oversight on cyber security, and the Department also participates on the NSC/HSC Interagency Policy Committee for the global information and communications infrastructure, a policy coordination group. DOE also has representation on a lower level interagency cyber security task force that is carrying forward some of the implementation planning from the previous Administration's Comprehensive National Cyber Security Initiative. Further, the Department's Office of Intelligence and Counter Intelligence is active within the intelligence community on cyber security coordination and planning.

Question 3. Currently, how are DOE and FERC coordinating with all of the other agencies and departments involved in cyber security (for example, DHS, DoD, and the Intelligence Community)?

Answer. Under HSPD 7, the Department serves as the lead federal agency for coordinating critical infrastructure activities in the energy sector, including cyber. In this capacity, the Department chairs the Energy Government Coordinating Council whose members include DHS, FERC, DHS, DOD, Nuclear Regulatory Commission, FBI, Natural Resources Canada (NRCan) et al. The Department participates with the intelligence community mainly through the DOE Office of Intelligence and Counterintelligence.

Question 4. How will these efforts be affected by the President's cybersecurity review?

Answer. Since the report on the President's 60-day cyber security review has not been issued, the Department cannot comment on the how the proposed efforts would be affected.

○