AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 617

111TH CONGRESS
2d Session

SENATE

REPORT
111–331

GRID RELIABILITY AND INFRASTRUCTURE DEFENSE ACT

SEPTEMBER 27, 2010.—Ordered to be printed

Mr. BINGAMAN, from the Committee on Energy and Natural Resources, submitted the following

R E P O R T

[To accompany H.R. 5026]

The Committee on Energy and Natural Resources, to which was referred the Act (H.R. 5026) to protect the bulk-power system and electric infrastructure critical to the defense of the United States against cybersecurity and other threats and vulnerabilities, having considered the same, reports favorably thereon with an amendment and recommends that the Act, as amended, do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. 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 systems and assets, whether physical or virtual, used for the generation, transmission., or distribution of electric energy affecting interstate commerce that, as determined by the Commission or the Secretary (as appropriate), are so vital to the United States that the incapacity or destruction of the systems and assets would have a debilitating impact on national security, national economic security, or national public health or safety.

"(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical infrastructure information 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 programmable electronic devices or com-

munications networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

"(5) CYBER SECURITY VULNERABILITY.—The term 'cyber security vulnerability' means 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.

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

"(b) AUTHORITY OF COMMISSION.—

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

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

"(3) CONSULTATION.—Before issuing a rule or order under paragraph (2), to the extent practicable, taking into account the nature of the threat and urgency of need for action, the Commission shall consult with the entities described in subsection (e)(1) and with officials at other Federal agencies, as appropriate, regarding implementation of actions that will effectively address the identified cyber security vulnerabilities.

"(4) TERMINATION OF RULES OR ORDERS.—A rule or order issued to address a cyber security vulnerability under this subsection shall expire on the effective date of a standard developed and approved pursuant to section 215 to address the 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 mitigate 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 Canada and Mexico responsible for the protection of cyber security of the interconnected North American electricity grid.

"(3) CONSULTATION.—Before exercising the authority granted under this subsection, to the extent practicable, taking into account the nature of the threat and urgency of need for action, the Secretary shall consult with the entities described in subsection (e)(1) and with officials at other Federal agencies, as appropriate, regarding implementation of actions that will effectively address the identified cyber security threat.

"(4) COST RECOVERY.—The Commission shall establish a mechanism that permits public utilities to recover prudently incurred costs required to implement immediate actions ordered by the Secretary under this subsection.

"(d) DURATION OF EXPEDITED OR EMERGENCY RULES OR ORDERS.—Any rule or order issued by the Commission without prior notice or hearing under subsection (b)(2) or any order issued by the Secretary 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 jurisdiction 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.

"(3) ALASKA AND HAWAII EXCLUDED.—Except as provided in subsection (f), nothing in this section shall apply in the State of Alaska or Hawaii.

"(f) DEFENSE FACILITIES.—Not later than 1 year after the date of enactment of this section, the Secretary of Defense shall prepare, in consultation with the Secretary, the States of Alaska and Hawaii, the Territory of Guam, and the electric

utilities that serve national defense facilities in those States and Territory, a comprehensive plan that identifies the emergency measures or actions that will be taken to protect the reliability of the electric power supply of the national defense facilities located in those States and Territory in the event of an imminent cybersecurity threat.

"(g) PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—

"(1) IN GENERAL.—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.).

"(2) RULES PROHIBITING DISCLOSURE.—Notwithstanding section 552 of title 5, United States Code, the Secretary and the Commission shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring cyber security under this section if the Secretary or Commission, as appropriate, decides disclosing the information would be detrimental to the security of critical electric infrastructure.

"(3) PROCEDURES FOR SHARING INFORMATION.—

"(A) IN GENERAL.—The Secretary and the Commission shall establish procedures on the release of critical infrastructure information to entities subject to this section, to the extent necessary to enable the entities to implement rules or orders of the Commission or the Secretary.

"(B) REQUIREMENTS.—The procedures shall—

"(i) limit the redissemination of information described in subparagraph (A) to ensure that the information is not used for an unauthorized purpose;

"(ii) ensure the security and confidentiality of the information;

"(iii) protect the constitutional and statutory rights of any individuals who are subjects of the information; and

"(iv) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.".

PURPOSE

The purpose of H.R. 5026 is to amend the Federal Power Act to protect the bulk-power system and critical electric infrastructure against cybersecurity threats and vulnerabilities.

BACKGROUND AND NEED

The electric infrastructure of the United States includes transmission lines, generation facilities, local distribution systems, and communications systems. As of 2009, there were 365,058 miles of transmission lines (rated 100 kV and above) in the United States, with an additional 31,000 miles of planned and conceptual additions forecast to be placed in service by 2019.[1] The total net summer generating capacity as of December 31, 2008, was 1,010,171 megawatts and 2008 annual net electric power generation was 4,119 million megawatt-hours.[2] This infrastructure serves over 143 million customers in the United States, across several sectors, including residential, commercial, and industrial. The components of the electric grid are highly interdependent, such that a line outage or system condition problems in one region can lead to reliability concerns in other regions.

On August 8, 2005, the Energy Policy Act of 2005 (EPAct) was enacted into law. Title XII of EPAct added a new section 215 to the Federal Power Act. Under section 215, the Federal Energy Regulatory Commission (FERC) is charged with overseeing mandatory,

[1] North American Electric Reliability Corporation, 2009 Long-Term Reliability Assessment 2009–2018 (October 2009) at 26.

[2] U.S. Energy Information, Administration Electric Power Annual 2008 (January 2010) DOE/EIA–0348 (2008)

enforceable reliability standards for the bulk power system. Section 215 also required FERC to select an Electric Reliability Organization (ERO) that is responsible for proposing reliability standards that are designed to protect and enhance the reliability of the bulk-power system and apply to users, owners, and operators of that system. The ERO is also authorized to impose penalties for violations of the reliability standards, subject to FERC review and approval. More than 1,800 different entities own or operate components of the bulk-power system that are subject to approved reliability standards.

In 2006, the FERC designated the North American Electric Reliability Corporation (NERC) as the ERO. In its capacity as the ERO, NERC is responsible for developing proposed reliability standards. The process of developing reliability standards relies on an inclusive and public process that permits extensive opportunity for industry comment. This process is intended to develop consensus on the need for, and the substance of, proposed standards. The standards development process includes the following key steps: nomination and public posting; industry review of comments; redrafting as necessary; formal balloting; and approval by NERC's board of trustees. Proposed standards are submitted to FERC for review and final approval. However, FERC cannot prescribe standards under section 215, but it has authority to direct NERC to develop standards or to modify existing standards.

The scope of the reliability standards is limited by section 215's definition of the bulk-power system, which specifically excludes "facilities used in the local distribution of electric energy." Accordingly, these standards do not apply to lower-voltage distribution facilities that serve critical electric infrastructure, such as certain defense facilities and other end-users of electricity. For example, this excludes virtually all of grid facilities in some large cities (e.g., New York), which precludes FERC action to mitigate cyber or other national security threats to reliability that involve such facilities in major population areas. In addition, the provisions of section 215 do not apply to Alaska or Hawaii, where a number of important defense facilities are located.

Standards relating to electric infrastructure cyber security represent one category of reliability standards. In August 2006, NERC submitted eight proposed cyber security standards, known as the Critical Infrastructure Protection (CIP) standards to FERC for approval under section 215. As defined by NERC for purposes of the CIP standards, critical infrastructure includes facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the electric system. NERC and its members worked for approximately three years to develop these standards before they were submitted to FERC for approval. In January 2008, FERC approved the CIP reliability standards while concurrently directing NERC to develop significant modifications addressing specific concerns. NERC addressed some of the FERC directives in subsequent versions of the cybersecurity standards. These revisions are effective April 1, 2010 and October 1, 2010, respectively. Notably, some entities were required to be fully compliant with all the CIP requirements as of July 1, 2010.

In addition to proposing new standards to FERC, NERC also reviews and modifies existing reliability standards. For example, further revisions to cyber security standards have been proposed based on unsatisfactory results from industry surveys of critical asset identification. In a December 2008 self-certification study, NERC reported that only 29% of generation owners and operators reported identifying at least one critical asset; approximately 63% of transmission owners identified critical assets. NERC expressed its concern with these results but an April 2010 survey does not indicate improvement in coverage.

Public reports relating to cyber vulnerabilities of and threats to the electric grid have increased in recent years and have been the subject of several hearings in the 110th and 111th Congresses. Such threats may arise across the vast array of communicating devices on the grid, requiring rapid and often confidential responses. In 2007, in an experiment (dubbed "Aurora"), researchers from DOE and the Idaho National Laboratory demonstrated that an attacker could hack into the control system of an electric generator or other rotating equipment connected to the grid, causing severe physical damage to the equipment. The experiment raised the possibility that large, coordinated attacks could damage the nation's electric infrastructure, resulting in billions of dollars in damage that could take months to repair.

Electric grid vulnerabilities also present risks to U.S. defense assets. Much of the energy infrastructure upon which the Department of Defense depends is commercially owned. An October 2009 report by the Government Accountability Office concluded that of the Department of Defense's 34 most critical global assets, 31 rely on commercially operated electricity grids for their primary source of electricity.[3]

The NERC process of developing and approving standards is necessary but not sufficient to protect the system against specific and imminent threats, particularly in emergency situations. The standards development process is designed to rely on industry expertise with respect to specific problems with long histories and defined data. It is also structured so as to permit opportunities for industry and public comment. FERC can direct NERC to develop a reliability standard to address a particular matter, including cyber security threats or vulnerabilities, either via the regular process or under an expedited schedule. However, many cyber security events require quick responses and significant changes that are not necessarily based on operating experience. In circumstances involving a cyber security threat to reliability, there may be a need to act decisively in hours or days, rather than weeks, months, or years. Existing NERC processes for adoption of reliability standards do not offer a timely means of responding to imminent cyber security threats and vulnerabilities.

LEGISLATIVE HISTORY

Representative Markey introduced H.R. 5026 on April 14, 2010. The House Committee on Energy and Commerce ordered it favor-

[3] U.S. Government Accountability Office, Defense Critical Infrastructure: Actions Needed to Improve the Identification and Management of Electrical Power Risks and Vulnerabilities to DOD Critical Assets (Oct. 2009) (GAO–10–147).

ably reported with an amendment in the nature of a substitute on April 15, 2010. H. Rept. 111–493. The House of Representatives passed H.R. 5026 by voice vote on June 9, 2010.

At its business meeting on August 5, 2010, the Committee on Energy and Natural Resources ordered H.R. 5026 favorably reported with an amendment in the nature of a substitute. The committee amendment consisted of the text of section 301 of S. 1462, the American Clean Energy Leadership Act of 2009, which was considered by the Committee at a business meeting on May 19, 2009, and ordered reported as part of S. 1462 on June 17, 2009. The Committee held a hearing on a draft of the legislation on May 7, 2009. S. Hrg. 111–29.

COMMITTEE RECOMMENDATION

The Committee on Energy and Natural Resources, in open business session on August 5, 2010, by voice vote of a quorum present, recommends that the Senate pass H.R. 5026, if amended as described herein.

SECTION-BY-SECTION ANALYSIS

Section 1 amends Part II of the Federal Power Act (16 U.S.C. 824 et seq.) by adding a new section 224 to give the Secretary of Energy and the Federal Energy Regulatory Commission (the Commission) additional authority to protect critical electrical infrastructure against cyber security threats and vulnerabilities.

Section 224(a) defines key terms in the new section.

Paragraph (1) defines the term "critical electric infrastructure" to mean systems and assets (whether physical or virtual) used for the generation, transmission, or distribution of electric energy affecting interstate commerce (whether or not transmitted in interstate commerce) that 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. It is modeled on the definition of the term "critical infrastructure" in the Critical Infrastructures Protection Act of 2001, section 1016 of the USA PATRIOT Act (42 U.S.C. 5195c(e)).

Paragraph (2) defines the term "critical electric infrastructure information" to mean critical information relating to critical electric infrastructure.

Paragraph (3) defines the term "critical infrastructure information" by reference to the definition of the term in section 212 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 131).

Paragraph (4) defines the term "cyber security threat" to mean the imminent danger of an act that disrupts, attempts to disrupt, or poses a significant risk of disrupting the operation of programmable electronic devices or communications networks essential to the reliable operation of critical electric infrastructure. Section 224(a) does not separately define or qualify the term "act," which bears its ordinary dictionary definition of "a thing done," and thus may include acts of God resulting from uncontrollable forces of nature, such as a geomagnetic storm.

Paragraph (5) defines the term "cyber security vulnerability" to mean a weakness or flaw in the design or operation of any pro-

grammable electronic device or communication network that exposes critical electric infrastructure to a cyber security threat.

Paragraph (6) defines the term "Secretary" to mean the Secretary of Energy.

Section 224(b)(1) directs the Commission to issue rules or orders as necessary to protect critical electric infrastructure from cyber security vulnerabilities. Paragraph (2) permits the Commission to issue the rules or orders, without prior notice or hearing, if it determines that the rule or order must be issued immediately to protect against a cyber security vulnerability. Paragraph (3) directs the Commission, to the extent practicable, to consult with officials at other Federal agencies, and with entities subject to the jurisdiction of the Commission. Paragraph (4) provides that rules or orders issued under subsection (b) shall expire on the effective date of a standard developed and approved pursuant to section 215 of the Federal Power Act to address the vulnerability.

Section 224(c) authorizes the Secretary of Energy to require, if immediate action is necessary to protect against a cyber security threat, entities subject to the jurisdiction of the Commission to take actions to protect against the threat. Paragraph (2) encourages the Secretary to consult and coordinate with appropriate officials in Canada and Mexico. Paragraph (3) requires the Secretary, to the extent practicable, to consult with officials at other Federal agencies, and with entities subject to the jurisdiction of the Commission under this section prior to exercising the authority under this subsection. Paragraph (4) requires the Commission to establish a mechanism that permits recovery of prudently incurred costs required to comply with orders of the Secretary under this subsection.

Section 224(d) provides that orders or rules issued without prior notice or hearing under section 224 shall remain in effect for not more than 90 days unless the Commission gives interested persons an opportunity to submit written data, views or arguments and affirms, amends or repeals the rule or order.

Section 224(e) provides that any entity that owns, controls, or operates critical electric infrastructure shall be subject to the jurisdiction of the Commission for purposes of carrying out section 224, or applying enforcement authorities of the Federal Power Act with respect to section 224, but subsection (e) does not subject an electric utility or other entity to the jurisdiction of the Commission for any other purpose. Except as provided in subsection (f), the States of Alaska and Hawaii are exempted from provisions of section 224.

Section 224(f) provides for a plan to protect the electric power supply of the national defense facilities in the States of Alaska and Hawaii, and in the Territory of Guam.

Section 224(g)(1) provides that section 214 of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 133) shall apply to information submitted to the Commission or the Secretary either voluntarily or involuntarily under this section to the same extent as that section applies to information voluntarily submitted to the Department of Homeland Security under that Act (6 U.S.C. 131 et seq.). Paragraph (2) directs the Secretary and the Commission to issue regulations prohibiting disclosure of information that would be detrimental to the security of critical electric infrastructure. Paragraph (3) directs the Secretary and the Commission to estab-

lish procedures on the release of critical infrastructure information to entities subject to this section, to the extent necessary to enable the entities to implement rules or orders of the Commission or Secretary. The procedures shall limit dissemination of information, ensure security and confidentiality of information, protect constitutional and statutory rights, and provide data integrity through timely removal and destruction of obsolete or erroneous names and information.

COST AND BUDGETARY CONSIDERATIONS

The following estimate of costs of this measure has been provided by the Congressional Budget Office:

H.R. 5026—An act to amend the Federal Power Act to protect the bulk-power system and electric infrastructure critical to the defense of the United States against cybersecurity and other threats and vulnerabilities

H.R. 5026 would amend existing law regarding the regulation of facilities that transmit electric power. Under existing law, most of the standards governing the reliability of the electric power system are issued by the Electric Reliability Organization (ERO), subject to approval and enforcement by the Federal Energy Regulatory Commission (FERC). This act would direct FERC to issue standards regarding the security of computer networks used to facilitate electric power transmission (known as cybersecurity), which would remain in effect until the ERO adopts regulations for such matters. The bill also would direct the Department of Defense (DoD) to conduct a study of grid security in certain states and territories and establish procedures for responding to emergencies and protecting information related to cybersecurity.

Enacting this legislation would affect direct spending by the federal power agencies that would be subject to the new regulations and standards; therefore, pay-as-you-go procedures apply. Based on information from the Tennessee Valley Authority and Bonneville Power Administration, CBO estimates that any effects of the legislation on net direct spending would be negligible because the new standards would be similar to those currently followed by federal agencies as a result of other statutory directives. The act also would affect spending at FERC and DoD, which is controlled by annual appropriation acts. Assuming appropriation of the necessary amounts, CBO estimates that DoD's analyses of grid security would cost about $1 million. Any increase in FERC's administrative costs would have no net budgetary impact because the agency recovers 100 percent of its costs through user fees. CBO estimates that enacting this bill would not affect revenues.

H.R. 5026 would impose an intergovernmental and private-sector mandate as defined in the Unfunded Mandates Reform Act (UMRA). The act would authorize FERC to issue rules and standards to protect the electric power system from cyber threats. Public and private entities that generate, transmit, or distribute electricity could be affected by those rules or standards. The costs of the mandate could be significant but would depend on future regulations. Consequently, CBO cannot determine whether the costs of the mandate would exceed the annual threshold for private-sector mandates ($141 million in 2010, adjusted annually for inflation).

Because public entities own and operate a small fraction of the nation's electric power infrastructure, CBO expects that the costs of the mandate would fall below the annual threshold established in UMRA for intergovernmental mandates ($70 million in 2010, adjusted annually for inflation).

CBO has not reviewed provisions of the act that would provide FERC and the Secretary of Energy with expedited or emergency authority to protect the electric transmission grid from threats to those computer networks for intergovernmental or private-sector mandates. Section 4 of the Unfunded Mandates Reform Act excludes from the application of that act any legislative provisions that are necessary for national security. CBO has determined that those provisions fall within that exclusion.

On May 19, 2010, CBO transmitted a cost estimate for H.R. 5026, the Grid Reliability and Infrastructure Defense Act, as ordered reported by the House Committee on Energy and Commerce on April 15, 2010. The Senate version of this legislation would authorize fewer programs and regulatory measures than the House bill, resulting in a smaller cost than CBO estimated for the House bill.

The CBO staff contacts for this estimate are Kathleen Gramp (for federal costs), Ryan Miller (for the intergovernmental impact), and Amy Petz (for the private-sector impact). The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In compliance with paragraph 11(b) of Rule XXVI of the Standing Rules of the Senate, the Committee makes the following evaluation of the regulatory impact which would be incurred in carrying out H.R. 5026, as proposed to be amended.

H.R. 5026, as proposed to be amended, would authorize the Federal Energy Regulatory Commission to issue rules and orders necessary to protect critical electric infrastructure from cyber security vulnerabilities, and the Secretary of Energy to issue emergency orders to avert or mitigate cyber security threats.

(A) *Number of business regulated.* H.R. 5026, as proposed to be amended, would apply to "any entity that owns, controls, or operates critical electric infrastructure, which the bill defines, in pertinent part, to include "systems and assets . . . used for the generation, transmission, or distribution of electric energy affecting interstate commerce that . . . 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." The Committee believes that, if the Commission determines that a rule or order is necessary, it could affect a large part of the nation's 3,273 electric utilities (including 210 investor-owned utilities, 2,009 publicly-owned utilities, 883 consumer owned rural electric cooperatives, and nine Federal electric utilities) and possibly some of the nation's 1,738 nonutility power producers.

(B) *Economic impact.* The economic impact of a rule or order could be significant, but would depend on the rule or order. The Committee notes that the Congressional Budget Office, in its report on S. 1462, stated that it expects the cost of any rule or order

issued under section 301 of S. 1462 (which is identical to H.R. 5026, as proposed to be amended) to be below the thresholds established under the Unfunded Mandates Reform Act ($69 million in 2009). In any event, the Committee expects any economic burden occasioned by the requirements to be offset by the potential damage to the electric grid and the disruption to the national economy that will be avoided by such emergency measures.

(C) *Personal privacy.* No personal information would be collected in administering the program. Therefore, there would be no impact on personal privacy.

(D) *Paperwork requirements.* Although the Commission or the Secretary may require the submission of some critical electric infrastructure information, the Committee does not expect the amount of information collected to impose substantial additional paperwork or recordkeeping burdens, in either time or financial cost, on private industry or individuals.

CONGRESSIONALLY DIRECTED SPENDING

H.R. 5026, as ordered reported, does not contain any congressionally directed spending items, limited tax benefits, or limited tariff benefits as defined in rule XLIV of the Standing Rules of the Senate.

EXECUTIVE COMMUNICATIONS

The testimony of the witnesses representing the Department of Energy and the Federal Energy Regulatory Commission at the Committee's May 7, 2009, hearing on draft cyber security legislation follows.

STATEMENT OF PATRICIA HOFFMAN, ACTING ASSISTANT SECRETARY, 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.

TESTIMONY 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 standards] using reasonable business judgment." Similarly, 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 dem-

onstrating 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 21 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.

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

[2] As an example, the U.S.-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.

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 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 infor-

mation 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 he happy to answer any questions you may have.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill H.R. 5026, as ordered reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

FEDERAL POWER ACT

The Act of June 10, 1920, Chapter 285, As Amended

Be it enacted by the Senate and the House of Representatives of the United States of America in Congress assembled,

* * * * * * *

PART II—REGULATION OF ELECTRIC UTILITY COMPANIES ENGAGED IN INTERSTATE COMMERCE

* * * * * * *

SEC. 223. JOINT BOARDS ON ECONOMIC DISPATCH.

* * * * * * *

(d) REPORT TO THE CONGRESS.—Within 1 year after enactment of this section, the Commission shall issue a report and submit such report to the Congress regarding the recommendations of the joint boards under this section and the Commission may consolidate the recommendations of more than one such regional joint board, including any consensus recommendations for statutory or regulatory reform.

SEC. 224. CRITICAL ELECTRIC INFRASTRUCTURE.

(a) DEFINITIONS.—In this section:

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

(2) CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—The term 'critical electric infrastructure information' means critical infrastructure information 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 programmable electronic devices or communications networks (including hardware, software, and data) essential to the reliable operation of critical electric infrastructure.

(5) CYBER SECURITY VULNERABILITY.—The term 'cyber security vulnerability' means 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.

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

(b) AUTHORITY OF COMMISSION.—

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

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

(3) CONSULTATION.—Before issuing a rule or order under paragraph (2), to the extent practicable, taking into account the nature of the threat and urgency of need for action, the Commission shall consult with the entities described in subsection (e)(1) and with officials at other Federal agencies, as appropriate, regarding implementation of actions that will effectively address the identified cyber security vulnerabilities.

(4) TERMINATION OF RULES OR ORDERS.—A rule or order issued to address a cyber security vulnerability under this subsection shall expire on the effective date of a standard developed and approved pursuant to section 215 to address the 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 mitigate 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 Canada and Mexico responsible for the protection of cyber security of the interconnected North American electricity grid.

(3) CONSULTATION.—Before exercising the authority granted under this subsection, to the extent practicable, taking into account the nature of the threat and urgency of need for action, the Secretary shall consult with the entities described in subsection (e)(1) and with officials at other Federal agencies, as appropriate, regarding implementation of actions that will effectively address the identified cyber security threat.

(4) COST RECOVERY.—The Commission shall establish a mechanism that permits public utilities to recover prudently incurred costs required to implement immediate actions ordered by the Secretary under this subsection.

(d) DURATION OF EXPEDITED OR EMERGENCY RULES OR ORDERS.—Any rule or order issued by the Commission without prior notice or hearing under subsection (b)(2) or any order issued by the Secretary 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 jurisdiction 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.

(3) ALASKA AND HAWAII EXCLUDED.—Except as provided in subsection (f), nothing in this section shall apply in the State of Alaska or Hawaii.

(f) DEFENSE FACILITIES.—Not later than 1 year after the date of enactment of this section, the Secretary of Defense shall prepare, in consultation with the Secretary, the States of Alaska and Hawaii, the Territory of Guam, and the electric utilities that serve national defense facilities in those States and Territory, a comprehensive plan that identifies the emergency measures or actions that will be taken to protect the reliability of the electric power supply of the national defense facilities located in those States and Territory in the event of an imminent cybersecurity threat.

(g) PROTECTION OF CRITICAL ELECTRIC INFRASTRUCTURE INFORMATION.—

(1) IN GENERAL.—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.).

(2) RULES PROHIBITING DISCLOSURE.—Notwithstanding section 552 of title 5, United States Code, the Secretary and the Commission shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring cyber security under this section if the Secretary or Commission, as appropriate, decides disclosing the information would be detrimental to the security of critical electric infrastructure.

(3) PROCEDURES FOR SHARING INFORMATION.—

(A) IN GENERAL.—The Secretary and the Commission shall establish procedures on the release of critical infrastructure information to entities subject to this section, to the extent necessary to enable the entities to implement rules or orders of the Commission or the Secretary.

(B) REQUIREMENTS.—The procedures shall—

(i) limit the redissemination of information described in subparagraph (A) to ensure that the information is not used for an unauthorized purpose;

(ii) ensure the security and confidentiality of the information;

(iii) protect the constitutional and statutory rights of any individuals who are subjects of the information; and

(iv) provide data integrity through the timely removal and destruction of obsolete or erroneous names and information.

* * * * * * *

○