Calendar No. 101

112TH CONGRESS
1st Session

SENATE

REPORT
112–34

GRID CYBER SECURITY ACT

JULY 11, 2011.—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 S. 1342]

The Committee on Energy and Natural Resources, having considered the same, reports favorably thereon, an original bill (S. 1342) 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, and recommends that the bill do pass.

PURPOSE

The purpose of the bill is to amend the Federal Power Act to protect the bulk-power system and critical electric infrastructure against cyber security 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 2010, there were 373,464 miles of transmission lines (rated 100 kV and above) in the United States, with an additional 33,000 miles of planned and conceptual additions forecast to be placed in service by 2018. The total net summer generating capacity as of October 2010, was 1,101,899 megawatts. 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 the EPAct added a new section 215

to the Federal Power Act. Under section 215, the Federal Energy Regulatory Commission (FERC or Commission) is charged with overseeing mandatory, enforceable reliability standards for the bulk power system.

Section 215 required FERC to select an Electric Reliability Organization (ERO) that is responsible for proposing reliability standards designed to protect and enhance the reliability of the bulk power system. These standards apply to over 1,900 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.

In 2006, 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. 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. FERC cannot prescribe standards under section 215, but it has authority to direct NERC to develop standards or to modify existing standards.

Currently, 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. For example, the current interpretation of bulk power system excludes virtually all of the grid facilities in certain large cities such as New York. In addition, the provisions of section 215 do not apply to Alaska or Hawaii, where a number of important federal installations 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. 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 directing NERC to develop significant modifications addressing specific concerns. NERC addressed some of the FERC directives in subsequent versions of the cyber security standards. These revisions were 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.

Public reports relating to cyber security vulnerabilities and threats have increased in recent years. In 2010, almost two-thirds of firms in the United States reported that they were the victim of cyber security incidents or information breaches, while the volume of malicious software on American networks more than tripled from 2009. Over the past five years, the number of incidents re-

ported by federal agencies to the United States Computer Emergency Readiness Team (US–CERT) increased from 5,503 incidents in fiscal year 2006 to about 41,776 incidents in fiscal year 2010. The commercial electric power grid increasingly faces threats that could lead to power disruptions. In July 2010, malicious software was discovered that appears to have been created specifically to attack industrial control systems widely used in electric power plants and at other important infrastructure. Since January 2010, NERC has issued 14 alerts to address a variety of cyber security-related issues and vulnerabilities.

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. The Department of Defense relies on commercial electric power for nearly 99% of its power needs at military installations.

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 structured 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

The bill builds on similar legislation developed by the Committee during the 111th Congress. The Committee held a hearing on draft cyber security legislation on May 7, 2009, considered the measure at a business meeting on May 19, 2009, and ordered it reported as section 301 of S. 1462, the American Clean Energy Leadership Act of 2009, on June 17, 2009. S. Hrg. 111–29; S. Rept. 11–48.

The House of Representatives passed a different measure, the Grid Reliability and Infrastructure Defense Act, H.R. 5026, by voice vote, on June 9, 2010. The Committee considered H.R. 5026 on August 5, 2010, and ordered it reported with an amendment in the nature of a substitute, which consisted of the text of section 301 of S. 1462. The Senate took no further action on S. 1462 or H.R. 5026 during the 111th Congress.

During the 112th Congress, the Committee held a hearing on a discussion draft of cyber security legislation on May 5, 2011. The discussion draft differed from section 301 of S. 1462 and the Committee amendment to H.R. 5026 in the previous Congress primarily in its reliance on NERC to develop reliability standards for cyber security pursuant to section 215 of the Federal Power Act, rather than authorizing FERC to impose cyber security requirements outside of section 215. In addition, following the May 5 hearing, the

Chairman and Ranking Member revised the discussion draft to clarify and restrict the application of cyber security requirements to certain critical distribution facilities and to provide for temporary emergency orders for cyber security vulnerabilities. The revised text further requires the Secretary of Energy to publish a report that assesses the susceptibility of critical electric infrastructure to electromagnetic pulse events and geomagnetic disturbances and directs FERC to assess the hardening of electric power transmission assets. The Committee ordered the revised discussion draft favorably reported at its May 26, 2011, business meeting.

COMMITTEE RECOMMENDATION

The Committee on Energy and Natural Resources, in open business session on May 26, 2011, by voice vote of a quorum present, recommends that the Senate pass an original bill, as described herein.

SECTION-BY-SECTION ANALYSIS

Section 1 sets forth the short title.

Section 2 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 Commission additional authority to protect critical electrical infrastructure against cyber security threats and vulnerabilities. The Committee intends that the Secretary or the Commission, as appropriate, will conduct outreach to the owners and operators of critical electric infrastructure in the implementation of their authorities.

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.

Paragraph (5) defines the term "cyber security vulnerability" to mean 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.

Paragraph (6) defines the term "Electric Reliability Organization" as having the meaning given the term in section 215(a).

Paragraph (7) defines the term "Secretary" to mean the Secretary of Energy.

Section 224(b)(1) directs the Commission, within 120 days after the date of enactment, to determine whether existing reliability standards are adequate to protect critical electric infrastructure from cyber security vulnerabilities. Paragraph (2) directs the Commission to order the ERO to submit a proposed reliability standard (or modification to a reliability standard) that adequately protects critical electric infrastructure from cyber security vulnerabilities if FERC finds the existing standards inadequate. Paragraph (3) grants the Commission authority to undertake the same determination and order steps following the issuance of an order under Paragraph (2) at any time after the initial determination. Given that general rulemaking requirements require that notices give "a description of the subjects or issues involved," the Committee expects that that orders from the Commission to the ERO will describe the subjects or issues involved in the cyber security vulnerabilities that are the subject of the order, so that the ERO can take appropriate action. Paragraph (4) provides that any reliability standard (or modification to a reliability standard) submitted pursuant to paragraph (2) or (3) will be developed in accordance with section 215 of the Federal Power. Paragraph (5) provides that the Commission may grant the ERO additional time to submit a proposed reliability standard or a modification to a reliability standard.

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 any order issued by the Secretary under subsection (c) shall remain in effect for not more than 90 days unless the Secretary 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 under this section, or developed by a Federal power marketing administration or the Tennessee Valley Authority under this section or section 215, 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 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 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.

Section 224(h)(1) provides that no person will have access to classified information relating to cyber security threats and vulnerabilities without appropriate security clearances. Paragraph (2) provides that Federal agencies and departments will cooperate with the Commission and Secretary in expeditiously providing security clearances to individuals that have a need-to-know classified information to carry out this section.

Section 3 amends section 215(a)(1) of the Federal Power Act to revise the definition of bulk power system for purposes of section 224. This revision expands the definition to include a limited number of facilities used in the local distribution of electric energy.

Section 4 amends section 215(i) of the Federal Power Act to limit the application of reliability standards and temporary emergency order to certain facilities used in the local distribution of electric energy. Such facilities are only to those that are so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health or safety.

Section 5 amends section 215(d) of the Federal Power Act to permit the Commission to require the ERO to develop and issue a temporary emergency order to address the cyber security vulnerability if the Commission determines that immediate action is necessary to protect critical electric infrastructure from a cyber security vulnerability.

Section 6 directs the Secretary of Energy, in consultation with appropriate experts at the National Laboratories, to conduct a study and publish a report that assesses the susceptibility of critical electric infrastructure to electromagnetic pulse events and geomagnetic disturbances. Within one year of the report's publication, the Commission is directed to assess whether and to what extent transmission infrastructure should be hardened against electromagnetic events and geomagnetic disturbances, including an estimate of the costs and benefits of options to harden the infrastructure. The Commission will do so in coordination with the Secretary of Energy and in consultation with electric utilities and the Electric Reliability Organization.

Section 7 specifies that for purposes of complying with the Statutory Pay-As-You-Go Act of 2010, the budgetary effects of this Act shall be determined by reference to the latest statement titled "Budgetary Effects of PAYGO legislation."

COST AND BUDGETARY CONSIDERATIONS

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

Grid Cyber Security Act

Summary: This legislation 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 bill would establish special procedures and deadlines for modifying the ERO's reliability standards if FERC determines that new guidelines are needed to protect the security of computer networks used to facilitate electric power transmission (known as cybersecurity). Other provisions would direct the Department of Energy (DOE) and the Department of Defense (DoD) to conduct studies on issues related to the security of the nation's electric power grid and would establish procedures for responding to emergencies and protecting information related to cybersecurity.

CBO estimates that implementing the bill would have a discretionary cost of $16 million over the 2012–2016 period, assuming appropriation of the necessary amounts. This legislation would affect direct spending by the federal power agencies that would be subject to any new cybersecurity standards; therefore, pay-as-you-go procedures apply. The legislation also could affect revenues and direct spending to the extent that it results in additional costs to the ERO. CBO estimates, however, that any effects of the legislation on net direct spending and revenues would be negligible.

The bill would impose intergovernmental and private-sector mandates, as defined in the Unfunded Mandates Reform Act (UMRA), on entities that transmit electric power. Because the costs to comply with those mandates would depend on future regulations, CBO cannot determine whether the aggregate cost of the mandate would exceed the annual threshold for private-sector mandates ($142 million in 2011, adjusted annually for inflation). Because public entities own and operate only a small fraction of the nation's electric power infrastructure, CBO expects that the aggregate cost of the mandate would fall below the annual threshold established in UMRA for intergovernmental mandates ($71 million in 2011, 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.

Estimated cost to the Federal Government: The estimated budgetary impact of this legislation is shown in the following table. The costs of this legislation fall within budget function 270 (energy).

	By fiscal year, in millions of dollars—					
	2012	2013	2014	2015	2016	2012–2016
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level	16	0	0	0	0	16
Estimated Outlays	3	6	7	0	0	16

Basis of estimate: For this estimate, CBO assumes that the legislation will be enacted by the end of fiscal year 2011 and the necessary amounts will be appropriated. Outlays are estimated to occur at historical rates for similar activities.

Spending subject to appropriation

Assuming appropriation of the necessary amounts, CBO estimates that implementing this bill would cost $16 million over the 2012–2016 period. Most of those costs would stem from provisions directing DOE to study the susceptibility of key electrical facilities to geomagnetic disturbances, such as solar flares, and electromagnetic pulses caused by natural or man-made sources. Based on information from DOE, CBO estimates that the cost of that assessment could range from about $10 million to $20 million, depending on the extent of any equipment purchases. For this estimate, CBO assumes that costs would be in the midpoint of that range and that the study would be completed within the three-year period specified in the bill. DoD's study of grid security in certain states and territories would cost about $1 million, CBO estimates.

Finally, CBO expects that implementing this legislation would expand FERC's workload and increase the agency's administrative expenses, which are controlled through annual appropriation acts. Because FERC recovers 100 percent of its costs through user fees, any such increases in its expenses would be offset by an equal change in fees that the commission charges, resulting in no net budgetary impact.

Direct spending and revenues

Taken together, the four federal power agencies own and operate about 15 percent of the nation's electric power, providing much of the transmission service in certain regions of the country. Spending by the Tennessee Valley Authority (TVA) and Bonneville Power Administration (BPA) constitutes direct spending because those agencies are authorized to collect and spend proceeds from the sale of electricity and to borrow funds to finance capital projects. Based on information from both agencies, CBO estimates that the net effect of the legislation on direct spending would be negligible because the new standards would probably be similar to those currently followed by federal agencies as a result of other statutory directives.

If FERC determines that new guidelines related to grid security are needed, the legislation also could expand the ERO's workload and increase its administrative costs. For purposes of the federal budget, the ERO is considered a governmental entity and its spending, which is not controlled by annual appropriation acts, is considered direct spending. The ERO derives its funding from fees

charged to users of the bulk-power system; those fees are considered revenues. Under the legislation, any increased direct spending by the ERO would generate a corresponding change in revenues to offset the entity's costs. Based on information from FERC and the ERO about current levels of spending related to grid security and the likely administrative costs involved with revising standards, CBO estimates that any increases in direct spending by the ERO and related revenues would not exceed $500,000 in any year.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. This legislation would affect net direct spending and revenues, but CBO estimates that any such effects would be negligible for each year and in total over the 2011–2021 period.

Intergovernmental and private-sector impact: The bill would impose intergovernmental and private-sector mandates as defined in UMRA by authorizing FERC to order the ERO to issue or modify standards to protect the electric power system from cyber threats. Any increase in administrative costs of the ERO would result in additional fees charged to public and private users of the bulk power system, but CBO estimates that any increase would not exceed $500,000 annually. Additionally, public and private facilities that transmit electric power could be affected by the standards issued or modified by the ERO. Because the costs to comply with those standards would depend on future regulations, CBO cannot determine whether the aggregate cost of the mandate would exceed the annual threshold for private-sector mandates ($142 million in 2011, adjusted annually for inflation). Because public entities own and operate only 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 ($71 million in 2011, 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.

Estimate prepared by: Federal costs: Kathleen Gramp and Megan Carroll; Impact on state, local, and tribal governments: Ryan Miller; Impact on the private sector: Amy Petz.

Estimate 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 the bill.

The bill would authorize the Federal Energy Regulatory Commission to order the Electric Reliability Organization (ERO) to develop additional reliability standards to provide adequate protection of

critical electric infrastructure from cyber security vulnerabilities. The additional standards would be applicable to owners, operators, and users of the bulk-power system. The Committee notes that the ERO already has authority to develop and enforce mandatory electric reliability standards for cyber security applicable to owners, operators, and users of the bulk-power system. The bill simply strengthens the Commission's authority to order the ERO to take further action if the Commission determines the ERO's standards are inadequate to protect the bulk-power system, and it expands the definition of the bulk-power system, for the limited purpose of protecting that system from cyber security vulnerabilities, to critical distribution facilities. The bill also gives the Secretary of Energy authority to issue emergency orders to avert or mitigate an imminent cyber security threat.

(A) *Number of businesses regulated.* The bill 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." Most of these entities are already subject to mandatory reliability standards developed and enforced by the ERO under section 215 of the Federal Power Act. The bill would, for the first time, make owners and operators of critical electric infrastructure used for the local distribution of electric energy subject to ERO standards, for the limited purpose of protecting the bulk-power system from cyber security vulnerabilities, but these entities may already be subject to ERO reliability standards as "users" of the bulk-power system.

(B) *Economic impact.* The economic impact of an ERO standard could be significant, but would depend on the standard. The Committee notes that the Congressional Budget Office, in its report on the Committee's amendment to H.R. 5026 (which is similar in scope to the proposed bill), stated that it could not determine whether the cost of compliance would exceed the annual threshold for private-sector mandates under the Unfunded Mandates Reform Act ($141 million in 2010), but expects the costs for public entities would fall below the annual threshold for intergovernmental mandates ($70 million for intergovernmental mandates in 2010). In any event, the Committee expects any economic burden occasioned by the requirements to be more than offset by the damage to the electric grid and the disruption to the national economy that will be avoided by any defensive measures required pursuant to the bill.

(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

The bill, as 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 provided by the Department of Energy and the Federal Energy Regulatory Commission at the May 5, 2011, Full Committee hearing follows:

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

Chairman Bingaman, Ranking Member Murkowski and members of the Committee, thank you for this opportunity to discuss the cyber security issues facing the electric industry, as well as proposed legislation intended to strengthen protection of the bulk power system and electric infrastructure from cyber security threats.

Title XIII of the Energy Independence and Security Act of 2007 (EISA) states, "It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure." The protection and resilience of critical national infrastructures is a shared responsibility of the private sector, government, communities, and individuals. As the complexity, scale, and interconnectedness of today's infrastructures have increased, it has changed the way services and products are delivered, as well as the traditional roles of owners, operators, regulators, vendors, and customers.

Ensuring a resilient electric grid is particularly important since it is arguably the most complex and critical infrastructure that other sectors depend upon to deliver essential services. Over the past two decades, the roles of electricity sector stakeholders have shifted: generation, transmission, and delivery functions have been separated into distinct markets; customers have become generators using distributed generation technologies; and vendors have assumed new responsibilities to provide advanced technologies and improve security. These changes have created new responsibilities for all stakeholders in ensuring the continued security and resilience of the electric power grid.

CYBER SECURITY ACTIVITIES AND ACCOMPLISHMENTS

For more than a decade, the Department of Energy's Office of Electricity Delivery and Energy Reliability (OE) has been substantively engaged with the private sector to secure the electric grid. In December 2003, the Homeland Security Presidential Directive 7 (HSPD–7) designated the Department as the sector-specific agency (SSA) for the energy sector responsible for collaborating with all federal

agencies, state and local governments, and the private sector. As the SSA, OE, representing the Department, works closely with the private sector and state/Federal regulators to provide secure sharing of threat information, to collaborate with industry to identify and fund gaps in infrastructure research, development and testing efforts, to conduct vulnerability assessments of the sector, and to encourage risk management strategies for critical energy infrastructure.

The 2010 *National Security Strategy* underscores the need to strengthen public-private partnerships in order to design more secure technology that will better protect and improve the resilience of critical government and industry systems and networks. OE has long recognized that neither government, nor the private sector, nor individual citizens can meet cyber security challenges alone. In 2006, OE facilitated the development of the *Roadmap to Secure Control Systems in the Energy Sector* to provide a detailed collaborative plan for improving cyber security in the energy sector and concrete steps to secure control systems used in the electricity and oil and natural gas sectors. The plan calls for a 10-year implementation timeline with a 5-year update scheduled for release in the summer of 2011. To implement the priorities in the *Roadmap*, the Energy Sector Control Systems Working Group was formed and comprised of cyber security and control systems experts from government, the electricity sector, and the oil and natural gas sector.

Since 2006, the *Roadmap* has provided a collaborative strategy for prioritizing cyber security needs and focusing actions under way throughout government and the private sector to ensure future energy system security. The *Roadmap* goals and strategy have also been fully integrated into the *Energy Sector-Specific Plan.* Since the *Roadmap* was released, important progress has been made in improving cyber security in the energy sector. These improvements have benefited existing systems and are contributing to the secure design and integration of advanced systems that incorporate smart grid technologies.

Through competitive solicitations and partnerships with industry, academia and national laboratories, OE has supported the development of several advanced cyber security technologies that are now commercially available within the energy sector:

- A technology to secure serial communications for control systems, based on the Secure Supervisory Control and Data Acquisition (SCADA) Communications Protocol developed by the Pacific Northwest National Laboratory. This technology is rapidly being adopted by utilities.
- Software toolkits, available for download from the vendor website, that let electric utilities audit the security settings of SCADA systems. The latest release addresses the Inter-Control Center Communications Protocol (ICCP), which is used for utility-to-utility communications.

• Monitoring modules that aggregate security events from a variety of data sources on the control system network and then correlate the security events to help utilities better detect cyber attacks.

• An Ethernet security gateway, based on an interoperable design developed by Sandia National Laboratories, that secures site-to-site Ethernet communications and protects private networks.

OE established the National SCADA Test Bed in 2003 to provide a national capability for cyber security experts to systematically evaluate the components of a functioning system for inherent vulnerabilities, develop mitigations, and test the effectiveness of various cyber security technologies. Major accomplishments include:

• Completed vulnerability assessments of 38 SCADA systems and provided mitigation recommendations. As a result, vendors have implemented many of the recommendations in "hardened" next-generation SCADA systems that are now commercially available and being deployed in the power grid.

• Utility groups have also formed partnerships to fund additional cyber security assessments at the test bed to address specific cyber security concerns.

• Provided advanced cyber security training for over 2300 representatives from over 200 utilities to demonstrate how to detect and respond to complex cyber attacks on SCADA systems.

• Developed the "Common Cyber Security Vulnerabilities Observed in Control System Assessments" report to help utilities and vendors mitigate vulnerabilities found in many SCADA systems. OE has also worked with the North American Electric Reliability Corporation (NERC) to develop the *Top Ten Vulnerabilities of Control Systems and their Associated Mitigations* report in 2006 and 2007.

OE is also working closely with academic and industry partners through the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG), which is a University led public-private research partnership supported by OE, Department of Homeland Security (DHS), and Industry for frontier research that supports resilient and secure smart grid systems. TCIPG leverages and expands upon previous research funded primarily by the National Science Foundation. TCIPG research focuses on building trusted energy delivery control systems from un-trusted components, and transitioning next-generation cyber security technologies to the energy sector. As an example, TCIPG released the Network Access Policy Tool that is now being used by industry and asset owners to characterize the global effects of local firewall rules in control system architectures. The tool will help utilities better manage and maintain security on their highly-complex communications networks.

Just recently, OE launched several new initiatives to enhance cyber security in the energy sector.

• OE, in coordination with DHS and other Federal agencies, has conducted several cyber threat information sharing workshops to analyze classified information, determine the impact to the sector, and develop mitigations that were specifically designed to work in the sector. This cooperative process has proven to be more effective and accepted than dictating solutions to the sector.

• OE, in coordination with the National Institute of Standards and Technology (NIST) and NERC, is leading a collaborative effort with representatives from across the public and private sectors to develop a cyber security risk management guideline. The objective of this effort is to provide a consistent, repeatable, and adaptable process for the electric sector, and enable organizations to proactively manage risk.

Ensuring the cyber security of a modern, digital electricity infrastructure is a key objective of national smart grid efforts. As a result, a number of key initiatives have been developed to ensure future system security and enable the energy sector to better design, build, and integrate smart grid technologies. OE has engaged in partnerships to perform these activities with key organizations including Federal Energy Regulatory Commission (FERC), the U.S. Department of Commerce, NIST, DHS, the Federal Communications Commission, the Department of Defense (DoD), the intelligence community, the White House Office of Science and Technology Policy, state public utility commissions, the National Association of Regulatory Utility Commissioners, NERC, the Open Smart Grid Subcommittee, Electric Power Research Institute (EPRI), and other energy sector organizations.

The American Recovery and Reinvestment Act of 2009 accelerated the development of smart grid technologies by investing in pilot projects, worker training, and large scale deployments. This public-private investment worth over $9.6 billion was dedicated to a nationwide plan to modernize the electric power grid, enhance the security of U.S. energy infrastructure, and promote reliable electricity delivery. The $4.5 billion in Recovery Act funds, managed by OE, was leveraged by $5.1 billion in funds from the private sector to support 132 Smart Grid Investment Grant and Smart Grid Demonstration Grant projects across the country. Each project awardee committed to implementing a cyber security plan that includes an evaluation of cyber risks and planned mitigations, cyber security criteria for device and vendor selection, and relevant standards or best practices the project will follow.

As called for in Section 1305 of EISA, OE is collaborating with NIST and other agencies and organizations to develop a framework and roadmap for interoperability standards that includes cyber security as a critical element. As part of this effort, NIST established the public-private Smart Grid Interoperability Panel, and within that, the 450-member Cyber Security Working Group (CSWG) to lead the development of cyber security require-

ments for the smart grid. After engaging members in numerous workshops and teleconferences and following two formal reviews, the CSWG released the first version of its "Cyber Security Guidelines for the Smart Grid". The three-volume document details a strategy that includes smart grid use cases, a high-level smart grid risk assessment process, smart grid-specific security requirements, development of a security architecture, assessment of smart grid standards, and development of a conformity assessment program for requirements.

To address cyber security needs for smart grid technologies, OE partnered with leading utilities and EPRI to develop cyber security profiles for major smart grid applications—Advanced Metering Infrastructure, Third-Party Data Access, and Distribution Automation. These profiles provide vendor-neutral, actionable guidance to utilities, vendors and government entities on how to build cyber security into smart grid components in the development stage, and how to implement those safeguards when the components are integrated into the power grid. These documents support the NIST "Cyber Security Guidelines for the Smart Grid" NISTIR—7628. OE also co-chairs the NIST CSWG.

SENATE ENERGY AND NATURAL RESOURCES COMMITTEE PROPOSED LEGISLATION

The proposed bill includes provisions intended to strengthen the bulk power system and electric infrastructure by addressing cyber security vulnerabilities and protecting against cyber security threats by adding a new section to the Federal Power Act (FPA). While the Administration does not yet have a position on the bill, the Department offers the following observations.

To begin with, the proposed bill correctly identifies, defines, and distinguishes between a cyber security vulnerability and a cyber security threat. These are two related, but different concepts. Vulnerabilities need to be identified and addressed, while threats need to be protected against. In that regard, references in the proposed bill to "protecting critical electric infrastructure from cyber security vulnerabilities" should be changed to "addressing critical electric infrastructure cyber security vulnerabilities."

In addition, Section 224(a)(1) defines critical electric infrastructure to include distribution assets that affect interstate commerce. This significantly expands FERC's jurisdiction for setting reliability standards beyond the bulk power system as provided in FPA section 215. Also, Section 224(f) would require a comprehensive plan identifying emergency measures to protect the reliability of the electric power supply of national defense facilities located in Alaska, Hawaii, and Guam in the event of an imminent cyber security threat. Pertinent to that, in July 2010, DOE and DoD signed a memorandum of understanding (MOU) "Concerning Cooperation in a Strategic Partnership to Enhance Energy Security". The purpose of the MOU is to en-

hance national energy security and demonstrate Federal Government leadership in transitioning America to a low carbon economy. This MOU provides an opportunity to develop a comprehensive approach that reduces the impact of power loss to defense critical assets, considering both mitigation and response measures to ensure vital defense capabilities are not disrupted.

Finally, the legislation does not yet address a unique, sensitive cyber security information disclosure problem faced by Federal Power Marketing Administrations subject to both the Freedom of Information Act and mandatory reliability standards enacted under Section 215 of the Federal Power Act. This sensitive information, developed under the mandatory reliability standards, appears not to be protected from public disclosure under the Freedom of Information Act. This security vulnerability could be avoided if legislation providing statutory protection for this information were enacted that qualified under Exemption 3 of the Freedom of Information Act.

CONCLUSION

In conclusion, I would like to again thank this Committee for its leadership in supporting the protection of the bulk power system and critical electric infrastructure against cyber security threats. Recognizing the interdependencies between different sectors, it is important to have a comprehensive strategy for cyber security legislation. DOE would be happy to work with the Committee on this legislation.

I would be pleased to address any questions the Committee might have.

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

My testimony summarizes the Commission's oversight of the reliability of the electric grid under section 215 of the Federal Power Act (FPA) and the Commission's implementation of that authority with respect to cyber security primarily through Order No. 706. I also will describe some of the current limitations in Federal authority to protect the grid against physical and cyber security threats, and also

comment on the cyber security discussion draft. The Commission currently does not have sufficient authority to require effective protection of the grid against cyber or physical attacks. If adequate protection is to be provided, legislation is needed and my testimony discusses the key elements that should be included in legislation in this area.

BACKGROUND

In the Energy Policy Act of 2005 (EPAct 2005), Congress entrusted the Commission with a major new responsibility to oversee mandatory, enforceable reliability standards for the Nation's bulk power system (excluding Alaska and Hawaii). This authority is in section 215 of the Federal Power Act. Section 215 requires the Commission to select an Electric Reliability Organization (ERO) that is responsible for proposing, for Commission review and approval, reliability standards or modifications to existing reliability standards to help protect and improve the reliability of the Nation's bulk power system. The Commission has certified the North American Electric Reliability Corporation (NERC) as the ERO. The reliability standards apply to the users, owners and operators of the bulk power system and become mandatory in the United States only after Commission approval. The ERO also is authorized to impose, after notice and opportunity for a hearing, penalties for violations of the reliability standards, subject to Commission review and approval. The ERO may delegate certain responsibilities to "Regional Entities," subject to Commission approval.

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

Limitations of section 215 and the term "bulk power system"

Currently, the Commission's jurisdiction and reliability authority is limited to the "bulk power system," as defined in the FPA, and therefore excludes Alaska and Hawaii, including any federal installations located therein. The current interpretation of "bulk power system" also excludes some transmission and all local distribution facilities, including virtually all of the grid facilities in certain large cities such as New York, thus precluding Commission action to mitigate cyber or other national security threats to reliability that involve such facilities and major population

areas. The Commission recently issued Order No. 743, which directs NERC to revise its interpretation of the bulk power system to eliminate inconsistencies across regions, eliminate the ambiguity created by the current discretion in NERC's definition of bulk electric system, provide a backstop review to ensure that any variations do not compromise reliability, and ensure that facilities that could significantly affect reliability are subject to mandatory rules. NERC is currently developing its response to that order. However, it is important to note that section 215 of the FPA excludes local distribution facilities from the Commission's reliability jurisdiction, so any revised bulk electric system definition developed by NERC will still not apply to local distribution facilities.

Critical infrastructure protection reliability standards

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

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

NERC filed the first phase of the modifications to the CIP Reliability Standards (Version 2) on May 22, 2009. In this phase, NERC removed from the standards the terms "reasonable business judgment" and "acceptance of risk," added a requirement for a "single senior manager" responsible for CIP compliance, and made certain other administrative and clarifying changes. In a September 30, 2009 order, the Commission approved the Version 2 CIP standards and directed NERC to develop additional modifications to certain of them. Pursuant to the Commission's September 30, 2009 order, NERC submitted Version 3 of the CIP standards which revised Version 2 as directed.

The Version 3 CIP standards became effective on October 1, 2010. This first phase of the modifications directed by the Commission in Order No. 706, which encompassed both Version 2 and Version 3, did not modify the critical asset identification process, a central concern in Order No. 706.

On February 10, 2011, NERC initiated the second phase of the Order No. 706 directed modification, filing a petition seeking approval of Version 4 of the CIP standards. Version 4 includes new proposed criteria to identify "critical assets" for purposes of the CIP reliability standards. This filing is currently under review by the Commission. In order to better understand the NERC Version 4 petition, particularly the number of critical cyber assets that will be identified under this revision, the Commission issued data requests to NERC, with responses due on July 11, 2011, which reflects an extension of time requested by NERC.

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

Identification of critical assets

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

When, in Order No. 706, the Commission approved Version 1 of the CIP reliability standards, it also required entities under those standards to self-certify their compliance progress every six months. In December 2008, NERC conducted a self-certification study, asking each entity to report limited information on its critical assets and the associated critical cyber assets identified in compliance with reliability standard CIP–002–1. As the Commission stated in Order No. 706, the identification of critical assets is the cornerstone of the CIP standards. If that identification is not done well, the CIP standards will be ineffective at pro-

tecting the bulk power system. The results of NERC's self-certification request showed that only 29% of responding generation owners and operators identified at least one critical asset, while about 63% of the responding transmission owners identified at least one critical asset. NERC expressed its concern with these results in a letter to industry stakeholders dated April 7, 2009.

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

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

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

THE NERC PROCESS

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

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

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

FERC rules governing review and establishment of reliability standards allow the agency to direct the ERO to develop and propose reliability standards under an expedited schedule. For example, FERC could order the ERO to sub-

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

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

This concern was highlighted in the Department of Energy Inspector General's January 2011 audit report on FERC's "Monitoring of Power Grid Cyber Security." The audit report identified concerns regarding the adequacy of the CIP standards and the implementation and schedule for the CIP standards, and concluded that these problems exist, in part, because the Commission's authority to ensure adequate cyber security over the bulk electric system is limited. The audit report concludes that the Commission should take a more aggressive action when ordering new or revised standards and highlights its lack of authority to implement its own reliability standards or mandatory alerts in response to emerging threats or vulnerabilities. This report emphasizes the need for FERC to have additional authority for ensuring adequate cyber security over the bulk electric system.

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

NERC's Formal Notices

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

SMART GRID

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

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

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

In regard to control systems, an attacker that gains access to the communication channels could order metering devices to disconnect customers, order previously shed load to come back on line prematurely, or order dispersed gen-

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

In addition to any smart grid related standards that may be adopted by the Commission, the CIP standards will apply to some, but not most, smart grid applications. The standards require users, owners and operators of the bulk power system to protect cyber assets, including hardware, software and data, which would affect the reliability or operability of the bulk power system. These assets are identified using a risk-based assessment methodology that identifies electric assets that are critical to the reliable operation of the bulk power system. If a smart grid device were to control a critical part of the bulk power system, it should be considered a critical cyber asset subject to the protection requirements of the CIP standards. However, this designation is currently up to the affected entity as part of its self-determination of critical cyber assets, as discussed previously.

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

PHYSICAL SECURITY AND OTHER THREATS TO RELIABILITY

The existing reliability standards do not extend to physical threats to the grid, but physical threats can cause equal or greater destruction than cyber attacks and the Federal government should have no less ability to act to protect against such potential damage. One example of a physical threat is an electromagnetic pulse (EMP) event. In 2001, Congress established a commission to assess the threat from EMP, with particular attention to be paid to the nature and magnitude of high-altitude EMP threats to the United States; vulnerabilities of U.S. military and civilian infrastructure to such attack; capabilities to recover from an attack; and the feasibility and cost of protecting military and civilian infrastructure, including energy infra-

structure. In 2004, the EMP commission issued a report describing the nature of EMP attacks, vulnerabilities to EMP attacks, and strategies to respond to an attack.[1] A second report was produced in 2008 that further investigated vulnerabilities of the Nation's infrastructure to EMP.[2] Both electrical equipment and control systems can be damaged by EMP.

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

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

---

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

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

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

The study assessed the 1921 solar storm, which has been termed a 1-in-100 year event, and applied it to today's power grid. The study concluded that such a storm could damage or destroy up to 300 bulk power system transformers interrupting service to 130 million people for a period of years.

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

THE NEED FOR LEGISLATION

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

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

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

Second, any legislation should allow the Commission to maintain appropriate confidentiality of sensitive information submitted, developed or issued under this authority. Without such confidentiality, the grid may be more vulnerable to attack and the Commission will not be able to adequately protect it. The cyber security discussion draft also includes provisions for protection of critical electric infrastructure information, which includes a provision for

FERC to establish procedures to allow the Commission to release critical infrastructure information to the extent necessary to enable entities to implement any FERC order under the proposal. It also appropriately would require FERC to limit redistribution of information so that the information is only in the hands of those that need to know.

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

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

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

In short, any new authority should allow the Commission to quickly order mandatory measures that are focused and confidential to address fast-moving, sophisticated and targeted cyber and physical attacks and natural events while providing cost recovery to the affected entities.

CONCLUSION

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

to testify today. I would be happy to answer any questions you may have.

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, 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. 215. ELECTRIC RELIABILITY.

(a) *DEFINITIONS*.—For purposes of this section:

[(1) The term]*(1) BULK-POWER SYSTEM*.—

(A) IN GENERAL.—The term "bulk-power system" means—

[(A)]*(i)* facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); [and]

[(B)]*(ii)* electric energy from generation facilities needed to maintain transmission system reliability [.]*; and*

(iii) for purposes of section 224, facilities used for the local distribution of electric energy that the Commission determines to be critical electric infrastructure pursuant to section 224.

[The term]*(B) EXCLUSION.—Except as provided in subparagraph (A), the term does not include facilities used in the local distribution of electric energy.*

(2) The terms "Electric Reliability Organization" and "ERO" mean the organization certified by the Commission under subsection (c) the purpose of which is to establish and enforce reliability standards for the bulk-power system, subject to Commission review.

* * * * * * *

(d) RELIABILITY STANDARDS.—(1) The Electric Reliability Organization shall file each reliability standard or modification to a reliability standard that it proposes to be made effective under this section with the Commission.

(2) The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission

shall give due weight to the technical expertise of the Electric Reliability Organization with respect to the content of a proposed standard or modification to a reliability standard and to the technical expertise of a regional entity organized on an Interconnection-wide basis with respect to a reliability standard to be applicable within that Interconnection, but shall not defer with respect to the effect of a standard on competition. A proposed standard or modification shall take effect upon approval by the Commission.

(3) The Electric Reliability Organization shall rebuttably presume that a proposal from a regional entity organized on an Interconnection-wide basis for a reliability standard or modification to a reliability standard to be applicable on an Interconnection-wide basis is just, reasonable, and not unduly discriminatory or preferential, and in the public interest.

(4) The Commission shall remand to the Electric Reliability Organization for further consideration a proposed reliability standard or a modification to a reliability standard that the Commission disapproves in whole or in part.

(5) The Commission, upon its own motion or upon complaint, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section.

(6) The final rule adopted under subsection (b)(2) shall include fair processes for the identification and timely resolution of any conflict between a reliability standard and any function, rule, order, tariff, rate schedule, or agreement accepted, approved, or ordered by the Commission applicable to a transmission organization. Such transmission organization shall continue to comply with such function, rule, order, tariff, rate schedule or agreement accepted, approved, or ordered by the Commission until

(A) the Commission finds a conflict exists between a reliability standard and any such provision;

(B) the Commission orders a change to such provision pursuant to section 206 of this part; and

(C) the ordered change becomes effective under this part.

If the Commission determines that a reliability standard needs to be changed as a result of such a conflict, it shall order the ERO to develop and file with the Commission a modified reliability standard under paragraph (4) or (5) of this subsection.

(7) TEMPORARY EMERGENCY ORDERS FOR CYBER SECURITY VULNERABILITIES.—Notwithstanding paragraphs (1) through (6), if the Commission determines that immediate action is necessary to protect critical electric infrastructure for a cyber security vulnerability, the Commission may, without prior notice or hearing, after consulting the ERO, require the ERO—

(A) to develop and issue a temporary emergency order to address the cyber security vulnerability;

(B) to make the temporary emergency order immediately effective; and (C) to keep the temporary emergency order in effect until—

(i) the ERO develops, and the Commission approves, a final reliability standard under this section; or

(ii) the Commission authorizes the ERO to withdraw the temporary emergency order.

* * * * * * *

(i) SAVINGS PROVISIONS.—(1) The ERO shall have authority to develop and enforce compliance with reliability standards for only the bulk-power system.

(2) This section does not authorize the ERO or the Commission to order the construction of additional generation or transmission capacity or to set and enforce compliance with standards for adequacy or safety of electric facilities or services.

(3) Nothing in this section shall be construed to preempt any authority of any State to take action to ensure the safety, adequacy, and reliability of electric service within that State, as long as such action is not inconsistent with any reliability standard, except that the State of New York may establish rules that result in greater reliability within that State, as long as such action does not result in lesser reliability outside the State than that provided by the reliability standards.

(4) Within 90 days of the application of the Electric Reliability Organization or other affected party, and after notice and opportunity for comment, the Commission shall issue a final order determining whether a State action is inconsistent with a reliability standard, taking into consideration any recommendation of the ERO.

(5) The Commission, after consultation with the ERO and the State taking action, may stay the effectiveness of any State action, pending the Commission's issuance of a final order.

(6) LIMITATION.—The ERO shall have authority to develop and enforce compliance with reliability standards and temporary emergency orders with respect to a facility used in the local distribution of electric energy only to the extent the Commission determines the facility is so vital to the United States that the incapacity or destruction of the facility would have a debilitating impact on national security, national economic security, or national public health or safety.

* * * * * * *

SEC. 223. JOINT BOARDS ON ECONOMIC DISPATCH.

(a) IN GENERAL.—The Commission shall convene joint boards on a regional basis pursuant to section 209 of this Act to study the issue of security constrained economic dispatch for the various market regions. The Commission shall designate the appropriate regions to be covered by each such joint board for purposes of this section.

(b) MEMBERSHIP.—The Commission shall request each State to nominate a representative for the appropriate regional joint board, and shall designate a member of the Commission to chair and participate as a member of each such board.

(c) POWERS.—The sole authority of each joint board convened under this section shall be to consider issues relevant to what constitutes "security constrained economic dispatch" and how such a mode of operating an electric energy system affects or enhances the reliability and affordability of service to customers in the region concerned and to make recommendations to the Commission regarding such issues.

(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) ELECTRIC RELIABILITY ORGANIZATION.—The term "Electric Reliability Organization" has the meaning given the term in section 215(a).

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

(b) AUTHORITY OF COMMISSION.—

(1) INITIAL DETERMINATION.—Not later than 120 days after the date of enactment of this section, the Commission shall determine whether reliability standards established pursuant to section 215 are adequate to protect critical electric infrastructure from cyber security vulnerabilities.

(2) INITIAL ORDER.—Unless the Commission determines that the reliability standards established pursuant to section 215 are adequate to protect critical electric infrastructure from cyber security vulnerabilities within 120 days after the date of enactment of this section, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than 180 days after the date of issuance of the order, a proposed

reliability standard or a modification to a reliability standard that will provide adequate protection of critical electric infrastructure from cyber security vulnerabilities.

(3) SUBSEQUENT DETERMINATIONS AND ORDERS.—If at any time following the issuance of the initial order under paragraph (2) the Commission determines that the reliability standards established pursuant to section 215 are inadequate to protect critical electric infrastructure from a cyber security vulnerability, the Commission shall order the Electric Reliability Organization to submit to the Commission, not later than 180 days after the date of the determination, a proposed reliability standard or a modification to a reliability standard that will provide adequate protection of critical electric infrastructure from the cyber security vulnerability.

(4) RELIABILITY STANDARDS.—Any proposed reliability standard or modification to a reliability standard submitted pursuant to paragraph (2) or (3) shall be developed and approved in accordance with section 215(d).

(5) ADDITIONAL TIME.—The Commission may, by order, grant the Electric Reliability Organization reasonable additional time to submit a proposed reliability standard or a modification to a reliability standard under paragraph (2) or (3).

(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 order issued by the Secretary under subsection (c) shall remain effective for not more than 90 days unless, during the 90 day-period, the Secretary—

(1) gives interested persons an opportunity to submit written data, views, or arguments; 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, or developed by a Federal power marketing administration or the Tennessee Valley Authority under this section or section 215, 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.

(h) ACCESS TO CLASSIFIED INFORMATION.—

(1) AUTHORIZATION REQUIRED.—No person shall be provided with access to classified information (as defined in section 6.1 of Executive Order 13526 (50 U.S.C. 435 note; relating to classified national security information)) relating to cyber security threats or cyber security vulnerabilities under this section without the appropriate security clearances.

(2) SECURITY CLEARANCES.—The appropriate Federal agencies or departments shall cooperate with the Secretary or the Commission, to the maximum extent practicable consistent with applicable procedures and requirements, in expeditiously providing appropriate security clearances to individuals that have a need-to-know (as defined in section 6.1 of that Executive Order) classified information to carry out this section.

○